ISO 9001:2015 – Implementing Risk Based Thinking

Denis J. Devos P.Eng
Advisor
Devos Associates Inc.
(519) 476-8951
Denis@DevosAssociates.com
www.DevosAssociates.com
Goal of this Session

- Discuss the new requirements for Risk Based Thinking
- Introduce Quantitative and Qualitative approaches to process risk
- Introduce a simple qualitative approach to Risk Assessment
Risk – It’s Obvious!

INTERNATIONAL CONFERENCE ON QUALITY STANDARDS
NOVEMBER 14 – 15, 2016
PITTSBURGH, PA
LEARN MORE

Devos Associates
Advisors to Industry
Risk is the Boogeyman
ISO 9001 Risk Definition

Effect of uncertainty

ISO 9000:2015 3.7.9

Effect of uncertainty on objectives

ISO 31000:2009 2.1
Requirements Related to Risk

5.1.2 Top Management shall demonstrate leadership and commitment with respect to customer focus by ensuring that:

b.) Risks & opportunities that can affect conformity of products/services and the ability to enhance customer satisfaction are determined & addressed.

4.4.1 The Organization shall determine the processes needed for the QMS and their application throughout the organization and shall determine ...

e.) The risks and opportunities in accordance with 6.1 and plan and implement the appropriate actions to address them.
6.1.1 When Planning for the QMS, the organization shall consider the issues referred to in 4.1 (Understanding the Organization and its Context), and 4.2 (Understanding the Needs of Interested Parties) and determine the risks and opportunities that need to be addressed to:

a.) Give assurance that the QMS can achieve its intended results

b.) Prevent, or reduce, undesired effects

c.) Achieve Continual Improvement
Requirements Related to Risk

6.1.2 The organization shall plan:

a.) **Actions** to address these risks & opportunities

b.) **How to:**
   - Integrate & implement actions into its QMS processes
   - Evaluate the effectiveness of these actions

Actions taken to address risks and opportunities shall be **proportionate** to the potential impact on the conformity of products and services.
9.3.1 Top Management shall review the organization’s QMS at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The **Management Review** shall be planned and carried out taking into consideration:

- d.) The effectiveness of actions taken to address Risks and Opportunities (see 6.1)
Requirements Related to Risk

6.1.2 NOTE:

Options to address risks/opportunities can include

• Avoiding Risk
• Taking Risk in order to pursue an opportunity
• Eliminating the Risk source
• Changing the likelihood or consequences
• Sharing the Risk
• Retaining Risk by informed decision
Risk Requirements - Guidance

It's clear that Risk-Based-Thinking has to begin with Top Management

- Clause 5.1.2 – Risks to Products/Services and Customer Satisfaction have to be determined and addressed.

- Clause 9.3.1 – Circle back via the Management Review to assess the effectiveness of actions taken to address Risks and Opportunities.
Risk Requirements - Guidance

It’s clear that Risk-Based-Thinking has to be embedded in the Processes

- Clause 4.4 – Determine Risks and Opportunities at the process level as processes are defined and then take appropriate actions to address

- Clause 6.1 – Consider Organizational context (vision and strategy) and the needs of stakeholders to identify risks to the business and mitigate them.
Levels of Organizational Risk

- Enterprise Risk
  - Regulatory environment
  - Market/Competitors Risk
  - Financial, Access to Capital Risk
- Product Risk
  - Product Safety
  - Early Failures, Reliability
- Operational Process Risk

It’s important to consider the above based on the type of business you are in. (The Organization and its Context, and needs of Interested Parties)
# Enterprise Risk - SWOT

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Strengths</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>People love our products</td>
<td>People love our products</td>
<td>Gov’t sales of new spectrum</td>
</tr>
<tr>
<td>We have strong supplier partners</td>
<td>We have strong supplier partners</td>
<td>New lower EMI requirements</td>
</tr>
<tr>
<td>Strong Marketing Division</td>
<td>Strong Marketing Division</td>
<td>Downward pressure on prices</td>
</tr>
<tr>
<td>We have great managers, engineers</td>
<td>We have great managers, engineers</td>
<td>Market shift to touchscreen tech.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lack of credit to upgrade capacity</td>
</tr>
<tr>
<td>Opportunity</td>
<td>Risk</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Lift Higher than any competitor</td>
<td>Safety - unit can tip over</td>
<td></td>
</tr>
<tr>
<td>New Colours And Decals</td>
<td>Colours can fade, not look good, decals wear off</td>
<td></td>
</tr>
</tbody>
</table>
Operational Controls

What are operational controls?

- What should they be?
- Where should they be?
- How big should they be?

We know that Operational Controls are appropriate when they are derived by and proportional to, RISK
Risk Assessment - Quantitative

There are a number of approaches to assessing risk quantitatively.

- Failure Modes and Effects Analysis (FMEA) considers the “three dimensions” of risk, Severity, Probability of Occurrence, and Effectiveness of Detection, in order to quantitatively prioritize risks for attention.
- Risk Matrix is simpler, which requires less detail and considers only Probability and Severity.
Risk Model - FMEA

Failure Modes and Effects Analysis

- Severity of the Failure (scale of 1-10)
- Probability of Occurrence (scale of 1-10)
- Effectiveness of Detection/Mitigation (1-10)

<table>
<thead>
<tr>
<th>Zone 1</th>
<th>Zone 2</th>
<th>Zone 3</th>
<th>Zone 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>What can go Wrong</td>
<td>How Severe is it?</td>
<td>How likely is it to happen?</td>
<td>Do we need improvement actions?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Process Function (Step)</th>
<th>Potential Failure Modes (Defects)</th>
<th>Potential Failure Effects</th>
<th>SEV</th>
<th>Class</th>
<th>Potential Causes of Failure</th>
<th>OCC</th>
<th>Current Process Controls</th>
<th>DET</th>
<th>RPN</th>
<th>Recommend Actions</th>
<th>Responsible Person &amp; Target Date</th>
<th>Taken Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Application Login</td>
<td>Login fails when correct credentials are entered</td>
<td>User cannot access account</td>
<td>8</td>
<td>C</td>
<td>Logic error/database error</td>
<td>4</td>
<td>Posts general error msg</td>
<td>1</td>
<td>32</td>
<td>Send urgent notice to DBA &amp; system administrator</td>
<td>Joe Josephson Release 4.2</td>
<td>In Process</td>
</tr>
<tr>
<td>2</td>
<td>Application Login</td>
<td>Login fails when correct credentials are entered</td>
<td>User cannot access account</td>
<td>10</td>
<td>N</td>
<td>External network failure</td>
<td>5</td>
<td>None</td>
<td>10</td>
<td>40</td>
<td>Talk to ISP about failover contract</td>
<td>Joe Josephson Release 4.2</td>
<td>Pending</td>
</tr>
<tr>
<td>3</td>
<td>Application Login</td>
<td>User cannot access another financial information</td>
<td>User cannot access another financial information</td>
<td>1</td>
<td>N</td>
<td>Logic error (different users can have same P#)</td>
<td>7</td>
<td>None</td>
<td>1</td>
<td>100</td>
<td>Include scenarios in test plan</td>
<td>Joe Josephson Release 4.2</td>
<td>In QA</td>
</tr>
</tbody>
</table>
Risk Model - FMEA

Consider creating an FMEA for every process identified in your QMS.

• Processes will be defined in accordance with Clause 4.4 of ISO 9001:2015. Flow charts are the preferred approach.

• Complete the header of the FMEA with the name of the process, the process owner, date, etc.

• PFMEA is most effectively accomplished with a small team. Convene a small team along with a customer and supplier of that process.
Risk Model - FMEA

Advantages

• Three Dimensions of Risk
• Failure Modes and Scoring on the same lines
• Quantitative, Scored
• Detailed and Rigorous

Disadvantages

• Quantitative, Scored
• Detailed and Rigorous
Risk Assessment - Quantitative

Another Approach is to use a Risk Matrix

- A two-dimensional chart plotting failure severity against likelihood of occurrence. Current Detection controls are not considered.

- 3 by 3 matrices can be used, but a 5 by 5 matrix is more common. Increasingly significant events are weighed more heavily than the last.

- As with FMEA, likelihood is the net result of the cause event and corresponding prevention controls.
# Risk Matrix

## 25th Annual ASQ Audit Division Conference: The Peabody Memphis

<table>
<thead>
<tr>
<th>Likelihood or Probability</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will Probably Occur</td>
<td>4 - Low Risk</td>
<td>8 - Moderate Risk</td>
<td>12 - High Risk</td>
<td>16 - Critical Risk</td>
<td>20 - Critical Risk</td>
</tr>
<tr>
<td><strong>4</strong> Probably will occur in most circumstances - 10%</td>
<td>4 - Low Risk</td>
<td>8 - Moderate Risk</td>
<td>12 - High Risk</td>
<td>16 - Critical Risk</td>
<td>20 - Critical Risk</td>
</tr>
<tr>
<td>Will Possibly Occur</td>
<td>3 - Low Risk</td>
<td>6 - Moderate Risk</td>
<td>9 - Moderate Risk</td>
<td>12 - High Risk</td>
<td>15 - High Risk</td>
</tr>
<tr>
<td><strong>3</strong> Might occur at some time - 1%</td>
<td>3 - Low Risk</td>
<td>6 - Moderate Risk</td>
<td>9 - Moderate Risk</td>
<td>12 - High Risk</td>
<td>15 - High Risk</td>
</tr>
<tr>
<td>Remote Possibility</td>
<td>2 - Low Risk</td>
<td>4 - Low Risk</td>
<td>6 - Moderate Risk</td>
<td>8 - Moderate Risk</td>
<td>10 - High Risk</td>
</tr>
<tr>
<td><strong>2</strong> Could occur in the future - 0.1%</td>
<td>2 - Low Risk</td>
<td>4 - Low Risk</td>
<td>6 - Moderate Risk</td>
<td>8 - Moderate Risk</td>
<td>10 - High Risk</td>
</tr>
<tr>
<td>Extremely Unlikely</td>
<td>1 - Low Risk</td>
<td>2 - Low Risk</td>
<td>3 - Low Risk</td>
<td>4 - Low Risk</td>
<td>5 - Moderate Risk</td>
</tr>
<tr>
<td><strong>1</strong> Only in exceptional circumstances 0.01%</td>
<td>1 - Low Risk</td>
<td>2 - Low Risk</td>
<td>3 - Low Risk</td>
<td>4 - Low Risk</td>
<td>5 - Moderate Risk</td>
</tr>
</tbody>
</table>
## Risk Matrix - Worksheet

### PROCESS RISK ASSESSMENT

<table>
<thead>
<tr>
<th>Step Number and Name</th>
<th>Risk</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Severity</th>
<th>Total</th>
<th>Risk Level</th>
<th>Action Required</th>
<th>Justification/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set-up a production machine</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. Raw Materials not available</td>
<td>Production Delay</td>
<td>3</td>
<td>3</td>
<td>9</td>
<td>Moderate</td>
<td>None</td>
<td>Increasing Raw Material on hand is expensive</td>
</tr>
<tr>
<td></td>
<td>2. Raw Materials poor quality</td>
<td>Customer Failures</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>High</td>
<td>Inspect Raw Materials</td>
<td>Cost of Failure is High</td>
</tr>
<tr>
<td></td>
<td>3. Inspector Not available</td>
<td>Production Delay</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>Low</td>
<td>None</td>
<td>Low Risk - Acceptable</td>
</tr>
<tr>
<td></td>
<td>4. Machine breakdown</td>
<td>Production Delay</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>Low</td>
<td>None</td>
<td>Low Risk - Acceptable</td>
</tr>
</tbody>
</table>

25th Annual ASQ Audit Division Conference: The Peabody Memphis
Risk Assessment - Qualitative

Unlike the Quantitative approach, a qualitative approach is based more on “gut feel” and does not follow a scoring guideline for determining where risk mitigation is required.

- This presentation uses a “Risk Assessment Table” as a way of capturing the thoughts and decisions of the group performing the assessment.
- This is the simplest approach, but the lack of numerical rankings can result in high inconsistency between groups performing assessments.
# Risk Assessment Table

## Process Name: Parts Production

<table>
<thead>
<tr>
<th>Interested Parties (Internal customers etc)</th>
<th>Their Needs</th>
<th>Process Name</th>
<th>Process Risks</th>
<th>Current Controls</th>
<th>Additional Controls Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Operation - Assembly Department</td>
<td>Parts on-time according to schedule, defect free</td>
<td>Step 1</td>
<td>Man (People)</td>
<td>Inspector not available</td>
<td>Set-ups are always the priority</td>
</tr>
<tr>
<td>Operations Management</td>
<td>Cycle times, yields, scrap/rework targets being met</td>
<td></td>
<td>Material</td>
<td>Material not available</td>
<td>Safety stock in the warehouse</td>
</tr>
<tr>
<td>External Customers - Users</td>
<td>Defect Free - High reliability</td>
<td></td>
<td>Method</td>
<td>Material is poor quality</td>
<td>Supplier Controls, inspections</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2 (Step Name)</th>
<th>Process Name</th>
<th>Process Risks</th>
<th>Current Controls</th>
<th>Additional Controls Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup Machine and perform</td>
<td>Man (People)</td>
<td>Machine is broken down</td>
<td>Preventive Maintenance</td>
<td>None</td>
</tr>
<tr>
<td>First Piece Inspection</td>
<td>Material</td>
<td>Measurement</td>
<td>Gage Preventive Maintenance</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3 (Step Name)</th>
<th>Process Name</th>
<th>Process Risks</th>
<th>Current Controls</th>
<th>Additional Controls Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run machine to product parts</td>
<td>Man (People)</td>
<td>Gage is broken/not available</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
Risk Assessment Table

The following briefly describes what belongs in each area of the Risk Assessment Table:

1. The header includes the process name, the needs of interested parties, and other information. Each process of the QMS should be examined for Risk.

2. Steps of the process (from the flowchart) should be listed here. Each step in the process can be examined for Risk.

3. In order to aid in the analysis, categories such as “5M” can be considered.
Risk Assessment Table

4. The group considers Risks for such categories as Man (people), Materials, Methods, Machines, Measurement etc. and lists them in this column.

5. Current Controls are those aspects of the process that are already in place to mitigate the risks in the prior column.

6. The last column lists the results of the review for that line and any actions that are decided upon for reducing Risks.
Risk Examples – Man (People)

- Lack of Skill/Experience
- Not enough people in place to do the job(s)
- No back-up person if the main person is on vacation
- No Succession planning for key positions
- Security concerns such as key cards for office doors, computer passwords, etc.
- Police Checks, Background checks for people in key positions
- Recruiting methods that may not identify the best candidates for new jobs
Risk Examples – Materials

- Running out of Raw Materials
- Losses due to shrinkage or disorganized warehouse
- Supply chain risks such as supplier capacity
- Supply chain risks such as long lead times for overseas suppliers etc.
- No back-up sources of supply for critical materials
- Poor quality of raw materials
- Lack of critical office supplies
- Distribution risks for finished goods
Risk Examples – Methods

• Lack of defined work Standards
• Lack of enforcement of Standards
• Methods that lead to poor outcomes
• Lack of contingency planning – defined reaction plans that are invoked when things go wrong
• Methods that are cumbersome or not user-friendly
• Lack of validation of Methods to prove that they are the most effective method
• Inefficient methods
Risk Examples – Machines

- Lack of state-of-the-art machinery leads to competitive disadvantage
- Lack of capability of machines
- Lack of maintenance of machines
- Lack of machine capacity
- Lack of machine/workplace safety
- Lack of IT, software, computer infrastructure
- Lack of workplace infrastructure such as desks, telephones, proper lighting, ergonomics etc.
Risk Examples – Measurement

- Insufficient inspection of outputs such as products or service outcomes
- Insufficient measurement devices for the above
- Lab/Inspection calibration risks
- Lack of follow-through on tasks and projects
- Lack of performance measurement for key business processes
- General lack of oversight and periodic review of processes and outputs, so that effective management is compromised.
ISO 9001:2015 – Implementing Risk Based Thinking

Denis J. Devos P.Eng
Advisor
Devos Associates Inc.
(519) 476-8951
Denis@DevosAssociates.com
www.DevosAssociates.com