Understanding Risk Based Thinking (RBT) In ISO 9001:2015

by Duke Okes

© 2015 Duke Okes

Why the Term “Risk Based Thinking”

- Preventive action clause was often misunderstood
- Need to be more proactive (as well as reactive)
- Part of trend towards risk based approach
- Avoid requiring formal risk management program

©2015 Duke Okes
Other Risk Based Applications

- DOE and graded approach
- FDA and risk based approach
- Banking & insurance
- Law firms
- Software testing
- Financial/GRC audits
- ...

Sort of similar to the Pareto principle … more effective allocation of resources!

Implementation of a QMS

Why are you doing these?

- Training
- Calibration
- Preventive maintenance
- Inspection
- Auditing
- ...

ISO 9001:2015 and Risk or “Risk-Based Thinking”

Introduction:
• Address risks and opportunities associated with context and objectives
• Employ process approach incorporating Plan-Do-Check-Act (PDCA) cycle and risk-based thinking
• Determine factors that could cause processes or QMS to deviate from planned results, put in place preventive controls to minimize negative effects and maximize opportunities
• Increase effectiveness of the QMS

ISO 9001:2015 and Risk or “Risk-Based Thinking”

4.4.1 QMS and its processes:
• Determine the processes needed for the QMS and address risks and opportunities per 6.1

5.1 Leadership and commitment:
• Promote the use of the process approach and RBT
• Ensure that risks and opportunities re: conformity of products and customer satisfaction are determined and addressed

6.1 Actions to address risks and opportunities:
• Plan and implement actions to address risks and opportunities and evaluate their effectiveness
• Actions should be proportionate to the potential impact on product conformity
9.1.3 Analysis and evaluation:
• Analyze and evaluate data from monitoring/measurement to evaluate effectiveness of actions taken to address risks and opportunities

9.3.2 Management review inputs:
• Management review shall consider effectiveness of actions taken to address risks and opportunities

10.2 Nonconformity and corrective action:
• When nonconformities/complaints occur the organization shall update risks and opportunities determined during planning, if necessary

A.4 Risk-based thinking:
• The concept of RBT has been implicit in previous editions of this standard via requirements for planning, review and improvement
• This edition requires the organization to understand its context and determine risks as a basis for planning
• This has allowed some reduction in prescriptive requirements in the standard and their replacement by performance-based requirements
• This provides greater flexibility in processes, documented information and organizational responsibilities
• There is no requirement for formal risk management or a documented risk management process
Some Common QMS Risk Assessments/Controls

- Contract review: Feasibility review
- Product/process design: FMEAs, validation testing
- Purchasing: Supplier selection (audits, samples)
- Production: Inspection, mistake-proofing, SPC
- Internal audit: Audit schedule prioritization
- Nonconforming material: Response based on risk
- Corrective action: Initiating/depth of investigations
- Management review: Monitoring system performance

Defining Context of the Organization

- External
  - Local, regional, national, international environments: Social, cultural, political, legal, regulatory, financial, technological, economic, natural and competitive
  - Key drivers and trends impacting on objectives
  - Relationships, perceptions and value of external stakeholders
- Internal
  - Governance, organizational structure, roles and accountabilities
  - Policies, objectives and strategies
  - Capabilities re: knowledge and resources (capital, time, people, processes, systems, technologies)
  - Information systems and flows, formal and informal decision making processes
  - Relationships, perceptions and value of internal stakeholders
  - Organizational culture [values and performance]
  - Standards, guidelines and models used
  - Format and extent of contractual relationships

From ISO 31000:2009, with 9001:2015 bold
Example Context

- Company: Manufacturer of black box audio simulator devices for highend guitar amplifiers
- Regulations: UL electronics codes, environmental on materials (solder)
- Customers: Small number, but major names
- Financials: High margin
- Workforce: 20-30, mostly young
- Facilities: Single facility in CO mountains, owned
- Processes: Program, stuff, wire, mold
- Competitors: None in product, but several similar companies in area
- Key employees: Design engineer, Sales manager
- Suppliers: US distribution companies

Stakeholder Analysis

<table>
<thead>
<tr>
<th>WHO ARE THEY</th>
<th>WHAT/WHY</th>
<th>HOW WELL DOING</th>
<th>ISSUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customers</td>
<td>Unique simulation capabilities</td>
<td>We're still the only significant player in the market</td>
<td>None</td>
</tr>
<tr>
<td>Regulators</td>
<td>Meet regs</td>
<td>No violations in last 3 years</td>
<td>None</td>
</tr>
<tr>
<td>Suppliers</td>
<td>Significant customer for them</td>
<td>Occasional difficulty getting key chips</td>
<td>Would be significantly impacted if not available</td>
</tr>
<tr>
<td>Employees</td>
<td>Opportunities to earn &amp; learn</td>
<td>No indications of problems, but key employees likely in high demand</td>
<td>Need to find ways to help them become a permanent part of the organization’s mission.</td>
</tr>
</tbody>
</table>
Example SWOT

<table>
<thead>
<tr>
<th>STRENGTHS</th>
<th>WEAKNESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Product unique function and performance</td>
<td>• Range of products and market</td>
</tr>
<tr>
<td>• Known as leader in development of new ideas</td>
<td>• Manual processes and skill levels</td>
</tr>
<tr>
<td>• Low debt</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPPORTUNITIES</th>
<th>THREATS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Expand to other amplifiers</td>
<td>• Environmental regulations</td>
</tr>
<tr>
<td>• Automation</td>
<td>• Drug laws</td>
</tr>
<tr>
<td>• Music industry trends toward live performances</td>
<td>• Loss of key employees with technical expertise and customer relationships</td>
</tr>
<tr>
<td></td>
<td>• Shortage of key chips</td>
</tr>
</tbody>
</table>

Risk Register

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Description</th>
<th>P</th>
<th>I</th>
<th>Risk</th>
<th>Mitigation</th>
<th>KRs</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Product - Component Supplier</td>
<td>Capacity of the industry</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>Consider design changes to utilize alternative components</td>
<td>Trends in lead time for orders</td>
<td><img src="green.png" alt="Green" /></td>
</tr>
<tr>
<td>2</td>
<td>HR</td>
<td>Loss of key employee</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>Retention contracts</td>
<td>Market demand for key positions</td>
<td><img src="yellow.png" alt="Yellow" /></td>
</tr>
</tbody>
</table>

©2015 Duke Okes
QMS Level RBT Process

- Quality Objectives
  - Context
  - Stakeholder Analysis
  - SWOT Analysis
  - Risk Register

ERM?
- Management Review
- Actions

RBT Should Obviously be Considered for Operations

- Contract review
- Product/process design
- External suppliers
- Production/service provision
- Release of products/services
RBT as a Performance Enhancer

How RBT Supports Effective Process Management

- PLAN – What risks might exist in the product/process, modify design to reduce those considered too high
- DO – Apply the controls defined during Planning, and be aware of other risks that might come about
- CHECK – Evaluate whether the controls are working, and whether there are indications of other risks not considered
- ACT – Modify the Plan where additional risks exist, and modify ineffective controls
## Assessing Risks of Each QMS Process

### TYPES OF RISK

<table>
<thead>
<tr>
<th>QMS Process</th>
<th>TYPES OF RISK</th>
<th>Specific Risks and/or Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Product Function</td>
<td>Delivery Performance</td>
</tr>
<tr>
<td>Probability</td>
<td>Impact</td>
<td>Risk</td>
</tr>
<tr>
<td>Customer contracting/ordering</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Product design</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Process design</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Purchasing</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

---

## Look at RM in Each QMS Process

- Is the need for RM being considered?
- For QMS processes where RM is deemed appropriate, is it being done adequately?
- Are controls aligned to RM findings?
- Does data indicate controls are effective?
- Are other risks being missed?
- Are risk events reported appropriately?
RM in the QMS

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer contracting/ordering</td>
<td>N</td>
<td>N</td>
<td>--</td>
<td>--</td>
<td>?</td>
<td>--</td>
</tr>
<tr>
<td>Product design</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Process design</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Purchasing</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Calibration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nonconforming material</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal audit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Note that a numeric scale could be used in place of Y/N/--)

RBT Flowchart for Plan & Do

1. Developing new (or change to) QMS, product, process or project
2. Is it likely to impact product quality, customer satisfaction or other quality objectives?
   - Yes
     - How significant could the impact be?
       - Minor
         - Use simple techniques such as brainstorming, C&E diagram, PHA, etc. to identify risks and any necessary controls
       - Major
         - Use more robust techniques such as FMEA, FTA, bow tie, Monte Carlo, etc. to identify risks and any necessary controls
   - No
     - Implement it
3. Follow up to evaluate results
RBT Flowchart for Performance Reviews (Check & Act)

Day-to-day operation of the QMS and its processes

Review of performance (inspection, test, performance metrics, audit, customer feedback, management review)

Is there an unacceptable variance in performance?

Were the designated controls in place?

Yes

No

Is there a need or opportunity to improve?

Yes

Consider initiating a CI project

No

No

Yes

Correct the controls

Consider whether root cause analysis should be conducted

Risk Ranking of Audit NCs

<table>
<thead>
<tr>
<th>NC Classification</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Severe impact on patient safety, extreme impact on public image</td>
</tr>
<tr>
<td>Major</td>
<td>High impact on patient safety, negative impact on public image</td>
</tr>
<tr>
<td>Moderate</td>
<td>Slight impact on patient and/or operations, unlikely impact on image</td>
</tr>
<tr>
<td>Minor</td>
<td>No measurable impact on patient, image of organization</td>
</tr>
</tbody>
</table>

Note: Higher classification NCs get reported higher in the organization
How Might ISO 31000 Help?

- Risk-based thinking requires risk-based understanding
- Provides terminology, principles and process to help assess and improve level of RBT
- Can simply be used as a reference/guide/info source, not a requirement
- And ISO 31010 can also be of value
  - Includes 31 different risk assessment techniques (~70 of 90 pages)
  - For each, gives overview, use, inputs & outputs, strengths and limitations

ISO 31000 RM Process Model

- Establishing the context
- Risk assessment
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment
- Monitoring and review
- Communication and consultation
Some Weak Process Examples

- FMEA information is often not shared with individuals responsible for the controls
- FMEAs are not used as part of root cause analysis
- FMEAs and other risk assessment tools are not reviewed (monitored) to determine their effectiveness

Some Potential Improvements

- Try some new techniques: ISO 31010 includes checklists, workshops, Bow tie, FMEA, fault tree, Monte Carlo … (31 in total)
- Calibrate everyone: Teach everyone the basic concepts of risk management, support reporting of risks & opportunities
- Make it more comprehensive: ISO 31000 risk management process includes context, communication and monitoring
So What’s Needed?

- Communication of:
  - Types of risks of concern (e.g., product quality, supply chain, compliance, cost of quality, reputational?)
  - Risk tolerance (application specific)
  - Responsibilities, processes and techniques for RBT

- Assessment of current RBT effectiveness

- Application and evidence of RBT

- Consider linking to ERM

Getting Started

- Develop context document
- Perform a SWOT analysis of the current QMS
- Provide training on RBT where needed
- Include RBT when planning/changing product/processes/organization
- Include RBT in management review
- Consider what evidence of RBT exists
Objective Evidence of RBT

- The processes and controls in place
- Output of risk assessments (e.g., checklists, FMEAs)
- Records (verbal or written) of decisions made regarding RBT (e.g., NCM, internal audit, corrective action, management review)

Difference Views of Risk

<table>
<thead>
<tr>
<th>Situations</th>
<th>Controls</th>
<th>Event</th>
<th>Controls</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software error</td>
<td>Testing</td>
<td>System slows down</td>
<td>Add resources</td>
<td>Frustration, higher cost</td>
</tr>
<tr>
<td>New technology</td>
<td>Validation</td>
<td>Unique location ID</td>
<td>Maintenance</td>
<td>Fewer errors, faster process</td>
</tr>
</tbody>
</table>

Performance Gains

- High
- Low

Opportunity Risks

- Low

Threat Risks

- High

Level of Risk Taking

- Low
Summary

- Understand context of the organization and how that impacts risks to achieving quality objectives
- Apply RBT at both the QMS and the process levels
- Provide leadership for implementation of risk-based thinking and related controls, and evaluate effectiveness

Contact Information

Duke Okes
423-323-7576
dokes@earthlink.net
www.aplomet.com