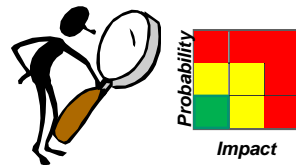


Understanding Risk Based Thinking (RBT) In ISO 9001:2015

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!

©2015 Duke Okes

Implementation of a QMS

Why are you doing these?

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

©2015 Duke Okes

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

©2015 Duke Okes

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

©2015 Duke Okes

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

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

©2015 Duke Okes

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

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

©2015 Duke Okes

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

©2015 Duke Okes

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***

©2015 Duke Okes

Example Context

- Company: Manufacturer of black box audio simulator devices for high end 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

©2015 Duke Okes

Stakeholder Analysis

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



©2015 Duke Okes

Example SWOT

<p>STRENGTHS</p> <ul style="list-style-type: none"> Product unique function and performance Known as leader in development of new ideas Low debt 	<p>WEAKNESSES</p> <ul style="list-style-type: none"> Range of products and market Manual processes and skill levels
<p>OPPORTUNITIES</p> <ul style="list-style-type: none"> Expand to other amplifiers Automation Music industry trends toward live performances 	<p>THREATS</p> <ul style="list-style-type: none"> Environmental regulations Drug laws Loss of key employees with technical expertise and customer relationships Shortage of key chips

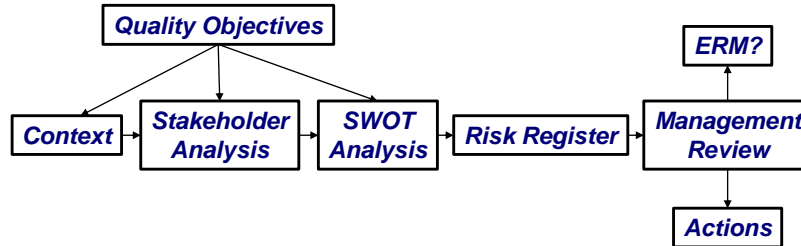
©2015 Duke Okes

Risk Register

ID	Type	Description	P	I	Risk	Mitigation	KRIs	Status
1	Product - Component Supplier	Capacity of the industry	M	H	H	Consider design changes to utilize alternative components	Trends in lead time for orders	
2	HR	Loss of key employee	H	H	H	Retention contracts	Market demand for key positions	

©2015 Duke Okes

QMS Level RBT Process



©2015 Duke Okes

RBT Should Obviously be Considered for Operations

- Contract review
- Product/process design
- External suppliers
- Production/service provision
- Release of products/services

©2015 Duke Okes

RBT as a Performance Enhancer



©2015 Duke Okes

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

©2015 Duke Okes

Assessing Risks of Each QMS Process

QMS Process	TYPES OF RISK												Specific Risks and/or Controls
	Product Function			Delivery Performance			Product Regulatory Compliance			Cost of Poor Quality			
	Probability	Impact	Risk	Probability	Impact	Risk	Probability	Impact	Risk	Probability	Impact	Risk	
Customer contracting/ordering	1	4	H	3	4	H	2	4	H	1	1	L	Not understanding customer application
Product design	4	5	H	1	2	M	4	4	H	5	5	H	Functionality, regulatory issues
Process design	2	4	H	3	3	M	1	3	M	5	5	H	Manufacturability
Purchasing	2	1	L	2	1	L	2	2	M	2	2	M	Control of regulated materials
Order fulfillment													
Calibration													
Nonconforming material													
Document control													
Internal audit													
...													

©2015 Duke Okes

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?

©2015 Duke Okes

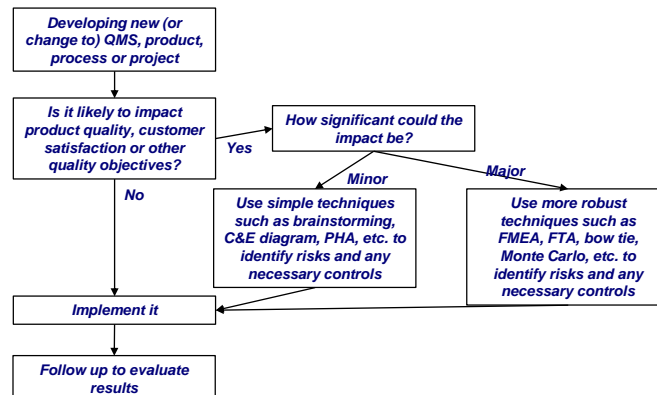
RM in the QMS

QMS Process	Risk Management Steps					
	RM Required?	RM Conducted?	Risks Identified?	Risks Mitigated?	Results Acceptable?	Events Reported?
Customer contracting/ordering	N	N	-	-	?	-
Product design	Y	Y	Y	Y	Y	Y
Process design	Y	Y	Y	Y	N	N
Purchasing	Y	Y	N	N	N	N
Order fulfillment						
Calibration						
Nonconforming material						
Document control						
Internal audit						
...						

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

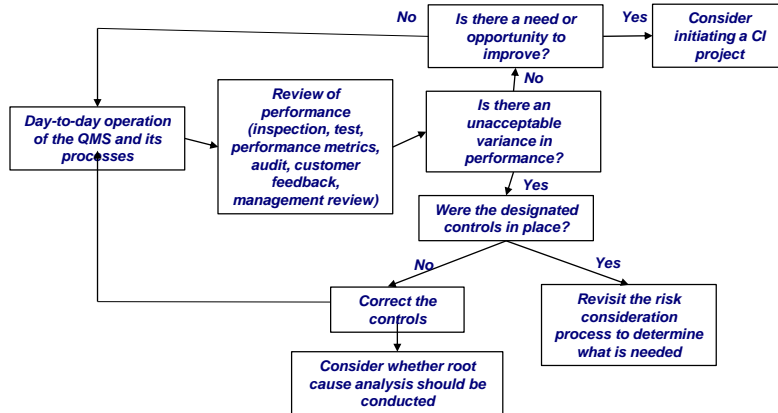
©2015 Duke Okes

RBT Flowchart for Plan & Do



©2015 Duke Okes

RBT Flowchart for Performance Reviews (Check & Act)



©2015 Duke Okes

Risk Ranking of Audit NCs

NC Classification	Criteria
Critical	Severe impact on patient safety, extreme impact on public image
Major	High impact on patient safety, negative impact on public image
Moderate	Slight impact on patient and/or operations, unlikely impact on image
Minor	No measurable impact on patient, image of organization

Note: Higher classification NCs get reported higher in the organization

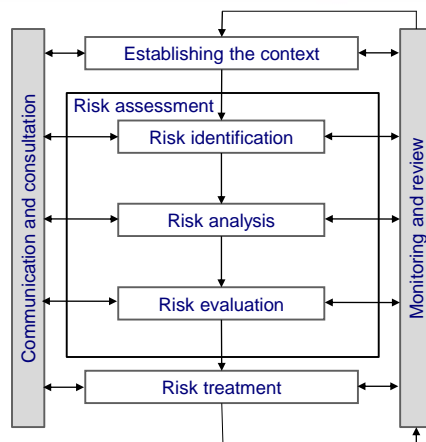
©2015 Duke Okes

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

©2015 Duke Okes

ISO 31000 RM Process Model



©2015 Duke Okes

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

©2015 Duke Okes

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

©2015 Duke Okes

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

©2015 Duke Okes

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

©2015 Duke Okes

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)

©2015 Duke Okes

Difference Views of Risk

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



©2015 Duke Okes

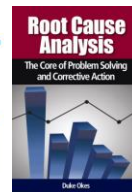
Summary

- 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

©2015 Duke Okes

Contact Information

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



APLOMET
Applied Logical Methods

Building Productive and Professional Organizations

©2015 Duke Okes