

11/10/2015

DMJ Miller & Assoc., Inc.



# Risky Business

Risk Based Thinking – A Proactive Approach

# ISO 9001 2015-09-15

## Quality Management systems - Requirements

### + New Concepts

- + Product  Product and Services
- + Documentation  Documented Information  
[Quality Manual, Documented Procedures, Records]
- + Purchased Products  Externally Provided  
Products & Services
- + Align the Quality Management Policy and Objectives with the Strategy of the Organization
- + Risk Based Thinking

ISO 9001 2015-09-15

## Quality Management systems - Requirements

### RISK BASED THINKING

- + Establishes a systematic approach to considering risk
- + Ensures that risks are identified, considered and controlled throughout the design, and use of the Quality Management System (QMS)
- + Consideration of risk is integral to the QMS
- + Proactive instead of reactive in preventing or reducing undesired effects. Preventive Action is "built in" to the QMS.

# Where is Risk Addressed in ISO 9001:2015?

## Introduction

- + 0.1 General – Potential benefits
  - + 0.1 c) Addressing risks and opportunities associated with its context and objectives.
- + 0.3 Process Approach
  - + 0.3.2 PDCA Cycle: PLAN – Identify and address risk and opportunities

## 0.3.3 Risk-based Thinking

- + Risk Based Thinking: Implicit in previous editions e.g.
  - + carrying out preventive action to eliminate potential nonconformities,
  - + analyzing nonconformities and taking action to prevent recurrence
- + Organization needs to: Plan and implement actions to address risk and opportunities.

# What Can Go Wrong?

## RISK

- + Potential of losing something of value, Resulting from a given action, activity and/or inaction
- + Intentional interaction with uncertainty



# Opportunity



- + A set of circumstances which makes it possible to do something.
- + Opportunity is not the positive side of risk
- + Taking or not taking an opportunity then presents different levels of risk.

# Where is Risk Addressed in ISO 9001:2015?

## 5 Leadership

- + Top management is required to:
  - + Promote awareness of risk-based thinking
  - + Determine and address risks and opportunities that can affect product/service conformity



# Where is Risk Addressed in ISO 9001:2015?

## 6 Planning

- + The organization is required to identify risks and opportunities related to QMS performance (Clauses 4.1 and 4.2) and take appropriate actions to address them.

## Where is Risk Addressed in ISO 9001:2015?

7 Support and 8 Operation no mention of risk-based thinking

However the organization is required to determine and provide necessary resources and manage its operational processes.

Risk is implicit whenever “suitable” or “appropriate” is mentioned in the clauses.

## Where is Risk Addressed in ISO 9001:2015?

### 9 Performance evaluation

- + The organization is required to monitor, measure, analyze and evaluate effectiveness of actions taken to address the risks and opportunities.

### 10 Improvement

- + The organization is required to correct, prevent or reduce undesired effects and improve the QMS and update risks and opportunities

## Where is Risk Addressed in ISO 9001:2015?

Everywhere!

By considering risk throughout the QMS and all processes

- + likelihood of achieving stated objectives is improved
- + Output is more consistent
- + Customers can be confident that they will receive the expected product or service

# Why use risk-based thinking?

- + Improves governance
- + Establishes a proactive culture of improvement
- + Assists with statutory and regulator compliance
- + Assures consistency of quality of products and services
- + Improves customer confidence and satisfaction

*Successful companies intuitively incorporate risk-based thinking*

# How do we use Risk-based thinking?

- + Identify what the risks are – within the context of the organization
- + Understand the risks – what is acceptable and unacceptable?
- + Plan Actions to address the risks
- + Check effectiveness of the action (or inaction)
- + Feedback from experience – collect data/information and adjust the plan as necessary.

# How do we use Risk-based thinking?

Types of risk –

## Organizational Risk

- + Occurs at the entity and activity level –
  - can be external – technology, competition, legislation
  - or internal – security, information systems, shipping and receiving, personnel competence
- + Affect individual units or functions

# How do we use Risk-based thinking?

## Types of Risk – Strategic

- + Organization Business Level
  - Inadequate business plan or strategy
  - Poor business decisions and/or execution
  - Inadequate resource allocation
  - Failure to recognize and respond to changes in the business environment



# How do we use Risk-based thinking?

## Types of Risk – Compliance

- + Failure to comply with Legal and Regulatory requirements
  - Conformance to quality regulations
  - Conformance to environmental standards and regulations
  - Health and safety requirements on site

# How do we use Risk-based thinking?

## Types of Risk – Operational

- + Organizational procedures, processes and actions
  - Management System Risk – Top Management ineffective, inefficient
    - Noncompliance with Financial rules
    - Human Resources practices
    - Marketing
    - Contract administration, Customer Communication
    - Design and Development

# How do we use Risk-based thinking?

## Type of Risk – Operational *continued*

- + Customer Satisfaction
  - Delivery of product
  - Design/repair of product
  - Inadequate response to customer feedback
  
- + Supply Chain
  - Outsourced products and services
  - Sole suppliers
  - Delivery on time

# How do we use Risk-based thinking?

## Types of Risk – Operational *continued*

### + Logistics

- Security on site
- Shipping Delays for security processes
- Damage during shipping

### + Natural Disasters

- Business Continuity - Safekeeping of information
- Disaster Recovery Plans (copies of the plan maintained offsite?)



11/10/2015

21

DMJ Miller & Assoc., Inc.

# Recap

- + ISO 9001:2015 new concepts
  - Risk-based thinking -the organization shall plan actions to address risk. There is no requirement for formal methods for risk management or a documented risk management process.
  - Implicit in the requirements for planning, review and improvement. Acts as a preventive tool.
  - Specified or implied throughout the standard
- + Why risk-based thinking
- + How to use risk-based thinking

# Recap

## + Types of Risk

- Organizational
- Strategic
- Compliance
- Operational
  - Management
  - Information Security
  - Customer Satisfaction
  - Logistics
  - Supply Chain
  - Natural Disaster
  - Revenue recognition

# Risk Analysis

## Risk Appetite

- + Amount of risk an entity is willing to accept – on a broad level
  - Measure of the Risk reward trade-off within the business
  - Tone set by top management

## Risk Tolerance

- + Related to the business specific objectives – Narrower focus
  - Amount of variation relative to the objectives an entity is willing to accept. Can vary within an organization's operating units



# Risk Analysis and Management

- + Risk Analysis Matrix
- + Controls –Entity Level
  - “Shall” statements
  - Policies
  - Code of Conduct
  - Communication Strategy
- + Controls – Activity Level
  - Documented information

# Risk Analysis and Management

- + Controls – Activity Level
  - Documented information
  - Control of production
  - Non-conforming products and services process
  
- + Mitigate Risk

# What Can Go Wrong?

## Risk Management Failures

- + Poor Governance and “Tone at the Top”
- + Reckless Risk Taking
- + Inability to Implement Enterprise Risk Management
- + Nonexistent, Ineffective or inefficient Risk Assessment



# What Can Go Wrong?

- + Falling Prey to a “Herd Mentality”
- + Misunderstanding the “If you can’t measure it, You Can’t Manage it” mindset
- + Accepting a lack of transparency in high Risk Areas
- + Not integrating Risk Management with Strategy-Setting and Performance Management
- + Ignoring the Dysfunctionalities and “Blind Spots” of the Organization’s Culture
- + Not involving the Board in a Timely Manner

# What Can Go Wrong?

- + General Motors Ignition Switch - Spectacular failure
  - Had an Enterprise Risk Management (ERM) System
    - Risk management was not inculcated into staff thinking and task performance
    - Not good at spotting, assessing and mitigating risk
  - Underestimated the original risk
  - No feedback loop of existing internal risk
  - Failed to recalculate inadequate cost benefit analysis
- ✧ Company's confidence in their ERM was misplaced

# What Can Go Wrong?

- + BP Deepwater Horizon April 2010
- + BP had previous disasters – i.e. refinery explosion in 2005, Ruptured pipeline 2006
- + CEO called for increased risk management but didn't deliver
- + Opted for cheaper and easier solutions (to save time and money)
- + Top management emphasizes exploration and production with little support for engineering excellence and maintenance budgets

# What Can Go Wrong?

- + Lack of effective communication. Safety concerns did not get to the right people.
- + No scenario planning for identified risks with no current solutions.
- + Board of Directors – were they uniformed or comfortable with the risk appetite?

**Risk Management isn't about avoiding risks.**

**Instead it is focused on understanding the key risk's a company faces**

**then taking the right risks at the best times**

**after using the most appropriate precautions**



# References

- + ISO 9001:2015, Quality management systems – Requirements
- + ISO BS EN 14971:2012 (E) Medical devices – Application of risk management to medical devices
- + International Organization for Standardization, *Risk-Based Thinking in ISO 9001:2015*
- + International Organization for Standardization, *ISO 9001:2008 to ISO 9001:2015, Summary of Changes*, ISO/TC176/SC 2/N1282
- + Eugene “Gene” A. Razzetti, *Two in One Risk strategy not only manages threats but also validates ISO standards programs*, Quality Progress, August 2010, ASQ
- + Paul Palmes, *A NEW Look, 15 things you must know about the upcoming ISO 9001 revision*, Quality Progress, September 2014, ASQ

## References *continued*

- + Sanford Liebesman, *Brought into Focus, ISO 9001:2015 specifically addresses risk. Is your organization ready?*, Quality Progress, September 2015, ASQ
- + Nicholas L. Squeglia, Expert Answers, *Minimizing risk*, Quality Progress, January 2010, ASQ
- + *Ten Common Risk Management Failures and How to Avoid Them*, The Bulletin, Volume 3 Issue 6, <http://www.protiviti.com/en-US/Pages/Ten-Common-Risk-Management-Failures-and-How-to-Avoid-Them.aspx>
- + *How Did BP's Risk Management Lead to Failure?*, ERM Initiative, July 2010, Poole College of Management, Raleigh NC
- + *As Cars Rely More Heavily on Computers, Risk of Hackers Grow*, Washington Post Blogs, July 15, 2015, Washingtonpost.Newsweek Interactive Company, LLC d/b/a Washington Post Digital.