A simple methodology for Risk Assessment

Miriam Boudreaux
CEO and Founder
Mireaux Management Solutions

ASQ
The Global Voice of Quality™
Introduction to Mireaux

We are a Technology and Consulting firm headquartered in Houston, TX.

Mireaux provides highly professional solutions to satisfy any organization's management improvement needs with a wide range of services, including:

- Consulting
- Internal Auditing
- Public and On-Site training
- Web QMS software
- Document Control
Training Objectives

• Gain an understanding of KEY TERMS

• Introduction to TYPES OF RISK and PURPOSE

• Risk IDENTIFICATION

• Overview of RISK ANALYSIS

• Intro to Risk CRITERIA & Risk EVALUATION
KEY TERMS Definitions

- Risk
- Risk Identification
- Risk Analysis
- Risk Criteria
- Risk Evaluation
- Risk Assessment
<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 14001</td>
<td>environmental problems with <strong>Pollution</strong></td>
</tr>
<tr>
<td>OHSAS 18001</td>
<td>safety problems with <strong>Injury &amp; Ill Health</strong></td>
</tr>
<tr>
<td>ISO 9001</td>
<td>quality problems with <strong>Product / Service</strong></td>
</tr>
<tr>
<td>API Q1, Q2</td>
<td></td>
</tr>
<tr>
<td>ISO 27001</td>
<td>security problems with <strong>Information</strong></td>
</tr>
</tbody>
</table>
There is no single method for determining [Significant Environmental Aspects], [Hazard prioritization].

The method used should provide consistent results and include establishing and applying evaluation criteria.
Although risks have to be identified and acted upon there is no requirement for formal risk management. (draft item 0.3)

When planning for the quality management system, the organization shall …
determine the risks and opportunities that need to be addressed to …
(6.1 Planning a-d)

Note: Options to address risks can include for example risk avoidance, risk mitigation or risk acceptance

…the organization shall determine, as appropriate,

b) actions to identify and address risks related to achieving conformity of goods and services to requirements;

8.3 Operational planning process
Risk As defined for **Quality** (API Spec Q1 9th Edition)

5.3 Risk Assessment and Management

… shall identify and control risk associated with impact on delivery and quality of product..

NOTE: Risk assessment can include consideration of severity, detection methods, and probability of occurrence.

5.5.2 Contingency Planning Output

…shall include, at a minimum:

a) actions required in response to significant risk scenarios to mitigate effects of disruptive incidents;

5.11 Management of Change

…shall identify the potential risks associated with the change
Risk As defined for **Quality** (API Spec Q2)

5.3 Risk Assessment and Management

… shall … control risk throughout the execution of a service.

5.5 Contingency Planning, 5.5.1 General

… shall include incident and disruption prevention and mitigation measures (...*in response to significant risk* scenarios 5.5.2.a).

5.11 MOC

…shall identify the potential risks (5.3) associated with the change

…shall conduct a risk assessment (5.3) when evaluating a potential change
Risk as defined for Information Security (27001)

As defined for Information Security (27001)

6.1.2 The organization shall define and apply an information security assessment process that:

a. Establishes and maintains security risk criteria that include:
   1. The risk acceptance criteria; and
   2. Criteria for performing information security risk assessments

b. Ensures that repeated information security risk assessments produce consistent, valid and comparable results;
Risk Management Process

- Establish the Type of Risk
- Identify the Risks
- Analyze the Risks
- Evaluate Risk Value against Criteria
  = Risk Value
- Understand the Process
- Establish Criteria

Risk Assessment
Understand the PROCESS

**INPUT**

- Web QMS Work Order
- Review Work Order
- Backup Restore
- Configuration
- Test
- Import Data
- Walk-Through
- Delivery and Training

**OUTPUT**

- Web QMS Deployed
- Give Client Log In Access
- Follow Up

Output from Preceding processes

Input to succeeding processes
# TYPES OF RISK

Management Systems are developed and used to control risks:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental Issues</td>
<td>ISO 14001</td>
</tr>
<tr>
<td>Health &amp; Safety Issues</td>
<td>OHSAS 18001</td>
</tr>
<tr>
<td>Quality Issues</td>
<td>ISO 9001, API Q1, API Q2</td>
</tr>
<tr>
<td>Information Security Issues</td>
<td>ISO 27001</td>
</tr>
</tbody>
</table>
Risk IDENTIFICATION

“finding, recognizing and describing risks”

Risk Identification

- involves the identification of risk sources, events
- their causes and their potential consequences
- can involve historical data, theoretical analysis
- informed and expert opinions

“What could go wrong”
Risk IDENTIFICATION

Environmental

New Web QMS Installation and Deployment

Technical Support
- Web QMS Work Order
- Review Work Order
- Backup Restore
- Configuration
- Test
- Import Data
- Give Client Log In Access
- Follow Up
- Web QMS Deployed

Software Developer

E-Learning Specialist

- Walk-Through
- Delivery and Training

Oil spill
CO₂ Emissions
Waste
Risk IDENTIFICATION

Health & Safety

- Fall Hazard
- Toxic inhalation
- Hearing Damage
Risk IDENTIFICATION

- Resin wrong blend
- OD too small
- Weld Fracture
Risk IDENTIFICATION

Information Security

Backup corruption

Data Loss

Hacking

New Web QMS Installation and Deployment

- Technical Support
  - Web QMS Work Order
  - Review Work Order
  - Backup Restore
  - Configuration
  - Test
  - Import Data
  - Give Client Log In Access
  - Follow Up
  - Web QMS Deployed

- Software Developer
  - Walk-Through
  - Delivery and Training

- E-Learning Specialist
  - Follow Up
RISK ANALYSIS Overview

process to comprehend the nature of risk and to determine the level of risk

In many cases this becomes a Qualification approach to Quantifying
RISK ANALYSIS Attributes

Identify Attributes of Risk, such as:

- Likelihood of Occurrence / Probability
- Criticality / Severity
- Detection

Establish Scale:

- 1 – 4, 1 – 5, 1 – 10?

Establish Scale Description for each attribute:

- 1- Low, 2 – Medium, 3- Average, etc.
- 1 – No impact, 2- Some impact, 3 – Big impact, etc.
### RISK ANALYSIS Scale

#### Possible Process-Related Approach

<table>
<thead>
<tr>
<th>Significance Scale</th>
<th>Scale of Impact</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Negligible</td>
<td>Very small impact. Low probability of occurrence</td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
<td>Impact and probability of occurrence are small</td>
</tr>
<tr>
<td>3</td>
<td>Serious</td>
<td>Could occur under normal operating conditions; impact is moderate with high probability of occurrence.</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>Could occur under normal operating conditions; impact is critical with high probability of occurrence.</td>
</tr>
</tbody>
</table>
Probability: The likelihood that the “event” will occur [aspect/impact]

1 = improbable
2 = remote (slight possibility of occurrence)
3 = moderate (50/50 chance of occurrence)
4 = probably will occur (difficult to predict when)
5 = very likely to occur
Severity: The Severity of Injury [hazard]

1 = Normal work can resume after basic first aid
2 = Lost time injury not reportable to Regulatory body
3 = Injury/Disease reportable to Regulatory body
4 = Fatality/Terminal Disease/major injury
5 = Multiple/Fatality
RISK ANALYSIS Scale

Severity: The Severity of failure mode [quality]

1 = will not cause any effect on operation and customer will probably not notice
2 = may result in minor rework – slight customer annoyance
3 = may cause unscheduled rework or repairs – some customer dissatisfaction
4 = may cause serious disruption to subsequent operations resulting in major rework – high degree of customer dissatisfaction
5 = involves breach of gov regs and may affect safe operation
RISK ANALYSIS

Scale

Severity: The Severity of Information Security Incidents

1. No impact on servers or data, no extra effort required to repair
2. Tangible harm to servers or data, extra effort required to repair
3. Significant expenditure of resources required. Damage to reputation and confidence
4. Compromise of large amounts of data or services
5. Permanent shutdown, complete compromise or servers or data, very difficult to go back to original state
**RISK ANALYSIS** Value

RISK VALUE = Severity x Probability x Detection

**Risk Analysis** Value can also be called:

- Risk Value
- **RPN**  Risk Priority Number
- Risk Level
- Level of Risk
### RISK ANALYSIS

<table>
<thead>
<tr>
<th>Process / Activity</th>
<th>Process Owner</th>
<th>Potential Risk</th>
<th>Severity</th>
<th>Probability</th>
<th>Detection</th>
<th>Risk Value</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machining</td>
<td>Mfg Mgr</td>
<td>Q Risk M1</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mfg Mgr</td>
<td>Q Risk M2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forklift</td>
<td>Whse Mgr</td>
<td>S Risk F1</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Waste Storage</td>
<td>Whse Mgr</td>
<td>E Risk W1</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drilling</td>
<td>Drilling Mgr</td>
<td>E Risk D1</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** for demo purposes ONLY - a Risk Matrix would contain only one Risk Type
Terms of reference against which the significance of a risk is evaluated.
# RISK CRITERIA

## Introduction

Begin by determining the maximum **Risk Level**:

<table>
<thead>
<tr>
<th>Based on 3 Risk Attributes</th>
<th>Max Risk Level</th>
<th>Risk Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scale</td>
<td>1 – 5</td>
<td>5 x 5 x 5</td>
</tr>
</tbody>
</table>

Then select the maximum **Risk** you will accept:

<table>
<thead>
<tr>
<th>Based on 3 Risk Attributes</th>
<th>Max Risk Level</th>
<th>Risk Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scale</td>
<td>1 – 5</td>
<td>5 x 5 x 5</td>
</tr>
</tbody>
</table>
# RISK CRITERIA

## Introduction

Severity x Probability x Detection = Risk Value  

Maximum Risk Value = \( 125 \)

Note: for demo purposes ONLY - a Risk Matrix would contain only one Risk Type

<table>
<thead>
<tr>
<th>Process / Activity</th>
<th>Process Owner</th>
<th>Potential Risk</th>
<th>Severity</th>
<th>Probability</th>
<th>Detection</th>
<th>Risk Value (S \times P \times D)</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machining</td>
<td>Mfg Mgr</td>
<td>Q Risk M1</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mfg Mgr</td>
<td>Q Risk M2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>Forklift</td>
<td>Whse Mgr</td>
<td>S Risk F1</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Waste Storage</td>
<td>Whse Mgr</td>
<td>E Risk W1</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Drilling</td>
<td>Drilling Mgr</td>
<td>E Risk D1</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>75</td>
<td></td>
</tr>
</tbody>
</table>
## RISK ANALYSIS Evaluation

<table>
<thead>
<tr>
<th>Process / Activity</th>
<th>Process Owner</th>
<th>Potential Risk</th>
<th>Severity</th>
<th>Probability</th>
<th>Detection</th>
<th>Risk Value</th>
<th>Criteria</th>
<th>Significant?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machining</td>
<td>Mfg Mgr</td>
<td>Q Risk M1</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>10</td>
<td>50</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Q Risk M2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>32</td>
<td>30</td>
<td>No</td>
</tr>
<tr>
<td>Forklift</td>
<td>Whse Mgr</td>
<td>S Risk F1</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>16</td>
<td>75</td>
<td>No</td>
</tr>
<tr>
<td>Waste Storage</td>
<td>Whse Mgr</td>
<td>E Risk W1</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>80</td>
<td>75</td>
<td>Yes</td>
</tr>
<tr>
<td>Drilling</td>
<td>Drilling Mgr</td>
<td>E Risk D1</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>75</td>
<td>75</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note: for demo purposes ONLY - a Risk Matrix would contain only one Risk Type
On Behalf of Miriam Boudreaux and Mireaux Management Solutions:

Thank YOU!