Internal Auditor Competency: So, How Will You Audit a Risk Assessment & Risk-Based Thinking?

Angelo Scangas
President, Quality Support Group, Inc

angelo@qualitysupportgroup.com

Quality Support Group, Inc.

Angelo Scangas - Presenter

Learning Objectives

- Effective techniques for auditing risk assessments
- Audit for compliance
- Audit for effectiveness

What is Risk?

- Risk is the possibility of events or activities impeding the achievement of an organization's strategic and operational objectives – ISO 31000

- Systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling and monitoring risk - ISO 14971

External/Internal
Environment
+
Interested Parties

Strategy
Objectives

Aligns Strategy and Execution

Systematically develops and
links plans from organizational
vision to operational tactics

QMS/BMS Scope
Products
Services

EFFECTIVENESS
OF PROCESS =
Ability to achieve
desired results

Input
Requirements Specified
(including resources)

Interrelated or interacting
activities and control
methods

Output
Requirements Satisfied
(result of the process)

Monitoring and Measuring

EFFICIENCY
OF PROCESS =
Results achieved
vs resources used

QMS

ACT PLAN
CHECK DO

Audit (Risk Based)

- Audit schedules should take into account "Risk" in developing an audit schedule and audit plan

- Risk can be due to :
  - New customer requirements
  - Supplier Issues
  - Technology
  - Regulations
  - Process changes
  - Material, equipment, etc.

Fundamental Risk Concepts (Annex C)

Risk:
Combination of the probability of occurrence of harm and the severity of that harm

Figure C.1 — Pictorial example of the relationship between hazard, sequence of events, hazardous situation and harm (from ISO/IEC Guide 63:2019[2])

Figure 1 — A schematic representation of the risk management process

Risk Analysis — 5
- Intended use and reasonably foreseeable misuse
- Identification of characteristics related to safety
- Identification of hazards and hazard situations
- Risk Estimation

Risk Assessment

Risk Evaluation — 6

Risk Control
- Risk control option analysis
- Implementation of risk control measure(s)
- Residual risk evaluation
- Benefit-risk analysis
- Risk arising from risk control measures
- Completeness of risk control

Risk Management Plan

Evaluation of overall residual risk

Risk management review — 9

Production and post-production activities — 10
- General
- Information collection
- Information review
- Actions

- Risk estimation = Severity x Occurrence and recorded in the risk file.
- A new medical device may not have sufficient information on occurrence
- Information on risk could be obtained from published standards, field data from similar devices, technical investigations, simulations, expert opinions.
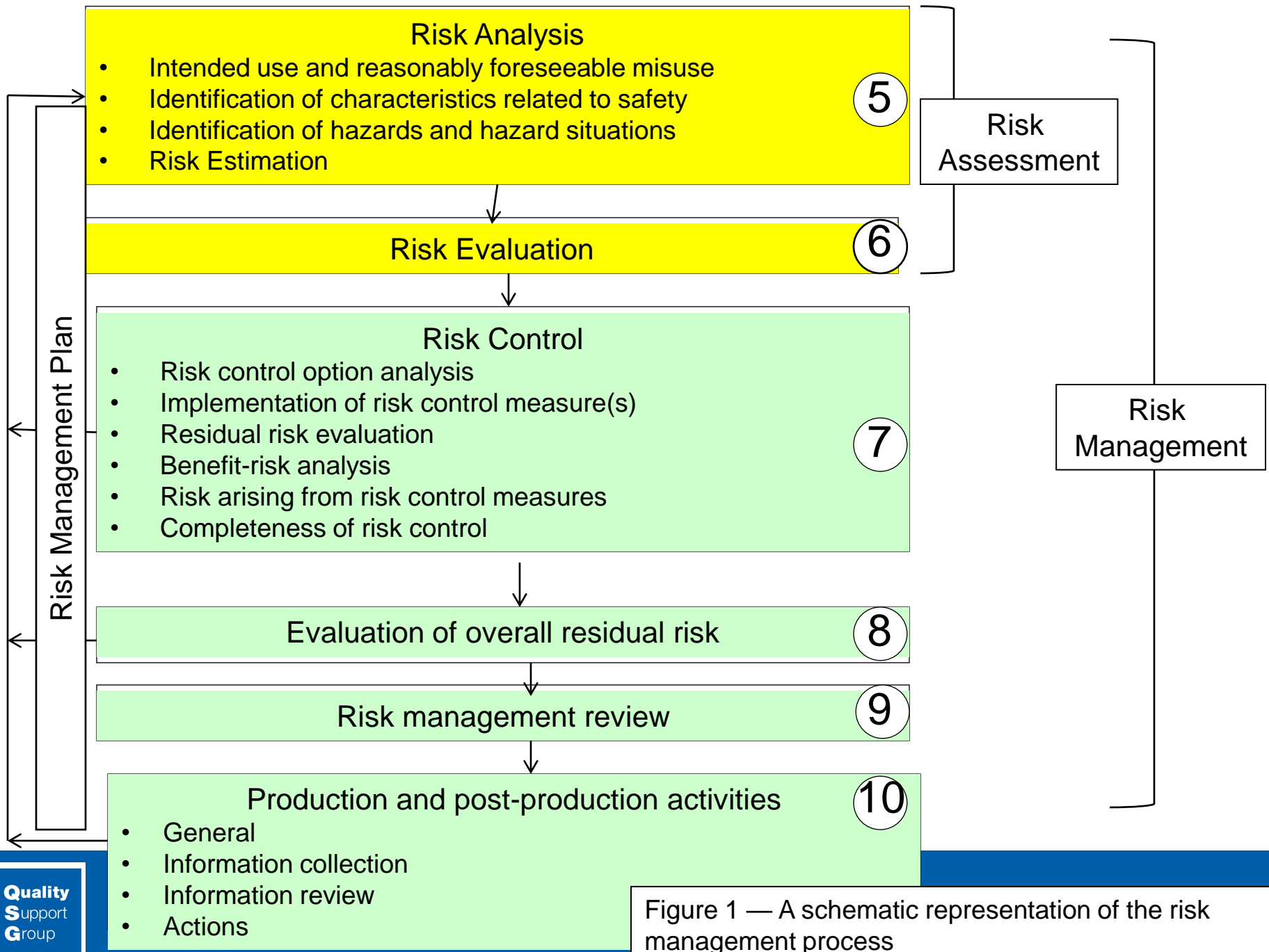- This should be recorded in the risk file

Figure 1 — A schematic representation of the risk management process

Quality Support Group

Materials
8.4 Externally provided
7.1.3 Infrastructure

Measures
9.1 Measurements
9.2 Internal Audit
9.3 Mgmt Review
4.3 Scope

Manpower
7.1.2 People
7.2 Competence
7.3 Awareness
6.2 Quality Objectives
5.2 Quality Policy
7.1.6 Organizational Knowledge
5.3 Org. Roles/Responsibilities

Inputs
8.2 Customer Requirements
4.4 QMS Requirements
4.1 Context
4.2 Interested Parties

Suppliers

Process
8.1,2,3,4,5,6 Operations

Outputs
8.6 Conforming products and services
8.5.5 Post Delivery Activities

Customers

ISO 9001:2015 Elements to Consider During a Process Audit

Methods
7.5 Documented Information

Machine
7.1.5 Monitoring and Measuring
7.1.3 Infrastructure

Environment
7.1.4 Environment
7.4 Communication
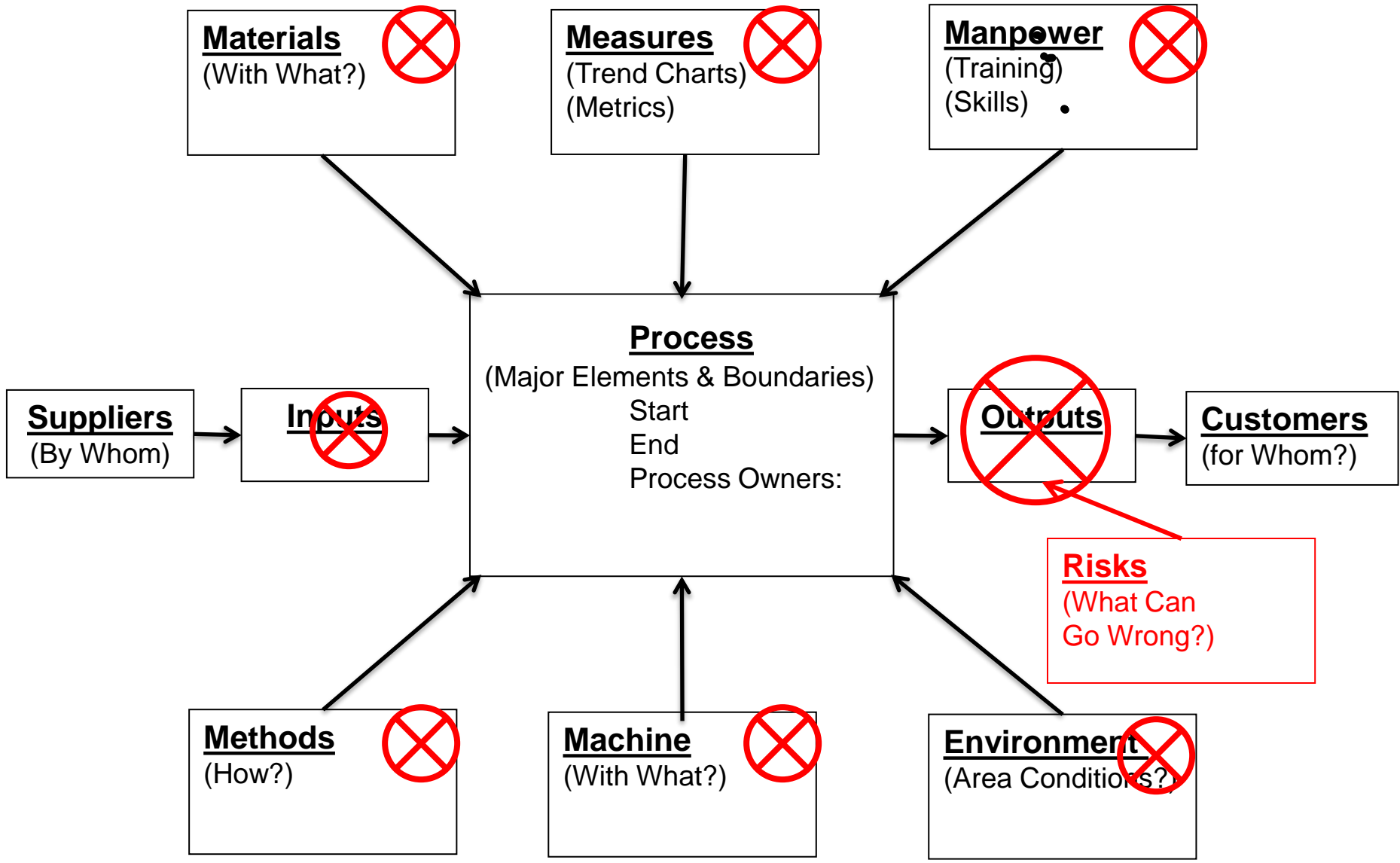
How do I Determine Risk for my Quality Management System?

How about Process Risk?

Materials
(With What?)

Measures
(Trend Charts)
(Metrics)

Manpower
(Training)
(Skills)

Process
(Major Elements & Boundaries)
Start
End
Process Owners:

Suppliers
(By Whom)

Inputs

Outputs

Customers
(for Whom?)

Risks
(What Can
Go Wrong?)

Methods
(How?)

Machine
(With What?)

Environment
(Area Conditions?)

Risk Assessments

1. **Risk Register**
   - Business Risk
   - Financial Risk
   - Project Risk
   - Etc.

2. **FMEA (Failure Modes and Effect Analysis)**

PROJECT RISK REGISTER

Project Oriented	Risk / Barrier / Obstacle / Constraint	Risk Likelihood	Risk Severity	Risk Owner	Action to Mitigate
Scope / Objectives					
Requirements / Deliverables					
Schedule					
Development Cost					
Quality					

				2) Risk Analysis:			3) Risk Response Planning:				1-Apr-08	RISK AFTER:	
1) Risk Identification:													
						TOTAL RISK: **104**							
Risk Item #	Entry Date	Process	Effect (Then this may happen…)	Probability (1 - 5)	Impact (1 - 5)	Risk Score (1 - 25)	Risk Owner	Response Type	Risk Mitigation Activities	Due Date		Estimated Probability After (1 - 5)	Estimated Impact After (1 - 5)
4.0	11-Jan-08	Development	Risk effect number 4	5	5	25	Sally Bobaly	Avoid	Risk Response 4.0	25-Jul-08		2	3
5.1	12-Mar-08	Supply Chain	Risk effect number 5	4	5	20	John Johnson	Mitigate	Risk Response 5.1	1-Aug-08		2	2
5.2						0	John Johnson	Contingency	Risk Response 5.2	2-Aug-08			
2.0	11-Jan-08	Project Mgmt	Risk effect number 2	5	3	15	Mary Jane	Contingency	Risk Response 2.0	1-Jun-08		2	1
8.1	19-Mar-08	Technical/ Design	Risk effect number 8	3	5	15	Jack White	Mitigate	Risk Response 8.1	15-Sep-08		3	1

Item / Process Step Function	Potential Failure Mode	Potential Effect(s) of Failure	S e v	C l a s s	Potential Cause(s)/ Mechanism(s) Of Failure	O c c u r	Current Process Controls		D e t e c	R P N	Recommended Actions	Response & Traget Complete Date	Action Results				
							Prevent	Detect					Action Taken	S E V	O C C	D E T	R P N

Key Concepts of Risk

- The <u>consequences/severity</u> (S) of that failure
  - how severe it might be to the stakeholders

- The <u>probability</u> (O) of occurrence of failure
  - how often the failure may occur

- The ability to <u>prevent</u> the failure/cause from occurring or <u>detect</u> the failure/cause (D) followed by action to prevent any effect on the stakeholders

Risk Assessment

- Severity (S)
- Occurrence (O)
- Detection (D)

Potential Risk (RPN) = S x O x D

Failure Modes & Effects Analysis (FMEA)

FMEA Timing

- Most effective when used <u>early</u> during product design and manufacturing process development.

FMEA Timimg

Origin of Failures

Elimination of Failures

Failures

FMEA

Into production

Time

POTENTIAL
FAILURE MODE AND EFFECTS ANALYSIS
Front Door L.H.

Item / Process Step / Function	Potential Failure Mode	Potential Effect(s) of Failure	S e v	C l a s s	Potential Cause(s)/ Mechanism(s) Of Failure	O c c u r	Current Process Controls		D e t e c	R P N	Recommended Actions	Response & Traget Complete Date	Action Results				
							Prevent	Detect					Action Taken	S E V	O C C	D E T	R P N

Item / Process Step / Function	Potential Failure Mode	Potential Effect(s) of Failure	S e v	C l a s s	Potential Cause(s)/ Mechanism(s) Of Failure	O c c u r	Current Process Controls		D e t e c	R P N	Recommended Actions	Response & Traget Complete Date	Action Results				
							Prevent	Detect					Action Taken	S E V	O C C	D E T	R P N
Critical	Anti-Function																

Quality Support Group, Inc.

Item / Process Step / Function	Potential Failure Mode	Potential Effect(s) of Failure	S e v	C l a s s	Potential Cause(s)/ Mechanism(s) Of Failure	O c c u r	Current Process Controls		D e t e c	R P N	Recommended Actions	Response & Traget Complete Date	Action Results				
							Prevent	Detect					Action Taken	S E V	O C C	D E T	R P N

Voice of the Customer

Severity Ranking

- Rating of 1 to 10 with 10 being the most severe impact.
  - Use a scale.
  - Use the same scale throughout.
- Assign severity rating for every possible effect.
  - Understand customer effects
  - Understand internal effects

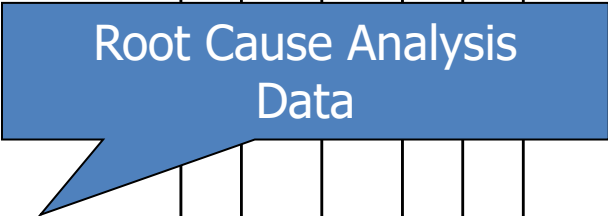 A Severity 9 or 10 must have preventive action

Item / Process Step / Function	Potential Failure Mode	Potential Effect(s) of Failure	S e v	C l a s s	Potential Cause(s)/ Mechanism(s) Of Failure	O c c u r	Current Process Controls		D e t e c	R P N	Recommended Actions	Response & Traget Complete Date	Action Results				
							Prevent	Detect					Action Taken	S E V	O C C	D E T	R P N

Root Cause Analysis Data

Quality Support Group, Inc.

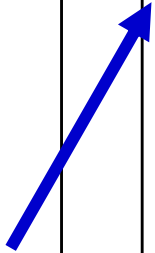| Item / Process Step / Function	Potential Failure Mode	Potential Effect(s) of Failure	S e v	C l a s s	Potential Cause(s)/ Mechanism(s) Of Failure	O c c u r	Current Process Controls		D e t e c	R P N	Recommended Actions	Response & Traget Complete Date	Action Results				
							Prevent	Detect					Action Taken	S E V	O C C	D E T	R P N

Occurrence Ranking

- How often will each potential cause occur?
  - Ignore the severity and the possibility that it will or will not be detected.
  - Rating of 1 to 10 with 10 being the most frequent occurrence.

- Use data where possible
  - C_{pk} information.
  - Customer complaints.
  - Corrective actions

- Occurrence - Need to consider the time frame for evaluation

Item/ Process Step / Function	Potential Failure Mode	Potential Effect(s) of Failure	S e v	C l a s s	Potential Cause(s)/ Mechanism(s) Of Failure	O c c u r	Current Process Controls		D e t e c	R P N	Recommended Actions	Response & Traget Complete Date	Action Results				
							Prevent	Detect					Action Taken	S E V	O C C	D E T	R P N

Think Prevention

Quality Support Group, Inc.

Item/Process Step / Function	Potential Failure Mode	Potential Effect(s) of Failure	S e v	C l a s s	Potential Cause(s)/ Mechanism(s) Of Failure	O c c u r	Current Process Controls		D e t e c	R P N	Recommended Actions	Response & Traget Complete Date	Action Results				
							Prevent	Detect					Action Taken	S E V	O C C	D E T	R P N

Quality Support Group, Inc.

Detection / Prevention Rating

- The assessment of the ability of the "process controls" to identify a potential cause or process weakness before the product is released to the customer.

- Rate the Detection from 1 to 10 with 10 being no chance of detecting the failure mode or cause.

Risk Estimation

- Each hazardous situation could have multiple possible harms ; all need to be identified.

- Risk= combination of probability of occurrence and the severity of that harm

Severity	Occurrence
Catastrophic	Frequent
Critical	Probable
Serious	Occasional
Minor	Remote
Negligible	Improbable

- Categories, like the ones above, can be interpreted differently by different individuals. Prior agreement prior to scoring is critical and will mitigate later discussions about which issues to address

888-336-1124 | www.qualitysupportgroup.com

DETECTION (D) Evaluation Criteria

Detection	Criteria: Likelihood of DETECTION by Design Control	Ranking
Absolute Uncertainty	**Design Control will not and/or can not detect a potential cause/mechanism and subsequent failure mode; or there is no Design Control.**	**10**
Very Remote	**Very remote chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.**	**9**
Remote	**Remote chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.**	**8**
Very Low	**Very low chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.**	**7**
Low	**Low chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.**	**6**
Moderate	**Moderate chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.**	**5**
Moderately High	**Moderately high chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.**	**4**
High	**High chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.**	**3**
Very High	**Very high chance the Design Control will detect a potential cause/mechanism and subsequent failure mode.**	**2**
Almost Certain	**Design Control will almost certainly detect a potential cause/mechanism and subsequent failure mode.**	**1**

6. Risk Assessment

- **Severity**

  The impacts) of failure

- **Occurrence**

  The likelihood of a failure occurrence from an identified

  cause under current controls

- **Detection**

  How detectable is the failure at any point?

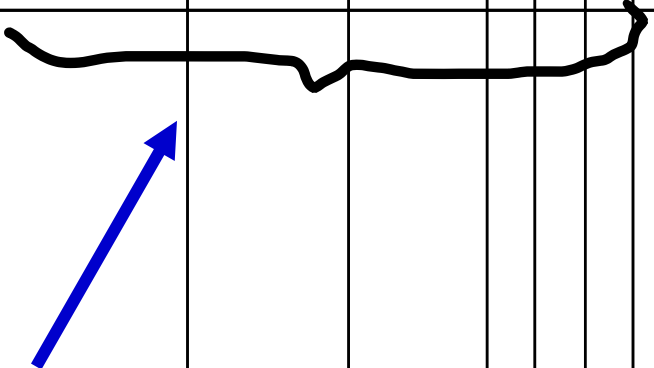**Potential Risk (RPN) = Severity x Occurrence x Detection**

Risk Estimation - Risk Matrix

	Improbable	Remote	Occasional	Probable	Frequent
Catastrophic	Medium	Medium	High	High	High
Critical	Medium	Medium	Medium	High	High
Serious	Low	Medium	Medium	Medium	High
Minor	Low	Low	Medium	Medium	Medium
Negligible	Low	Low	Low	Medium	Medium

NOTE: While one can categorize risks by severity and probability, all risk need to be reduced as far as possible (AFAP)

Quality Support Group

FMEA

Item / Process Step / Function	Potential Failure Mode	Potential Effect(s) of Failure	S e v	C l a s s	Potential Cause(s)/ Mechanism(s) Of Failure	O c c u r	Current Process Controls		D e t e c	R P N	Recommended Actions	Response & Traget Complete Date	Action Results				
							Prevent	Detect					Action Taken	S E V	O C C	D E T	R P N

RISK ASSESSMENTS ARE "LIVING" DOCUMENTS!

Need to be updated!
What are the "triggers" for updating?

In Conclusion

- ◈ Timing
- ◈ Team
- ◈ Process knowledge
- ◈ Control / Update
- ◈ Data-based decisions
- ◈ Justification for the criteria used
- ◈ Acceptability / Residual Risk
- ◈ Mitigation actions
- ◈ Effectiveness of actions taken

Quality **S**upport **G**roup

Thank you!

Questions?

Angelo Scangas
Angelo@QualitySupportGroup.com
978-430-7611
www.qualitysupportgroup.com