# A ñRisk Based Thinkingò Model for ISO 9001:2015

**Bob Deysher**

**Senior Consultant**

# Agenda

- Why implement Risk Based Thinking?
  - What does ISO 9001:2015 require?
- What is Risk Based Thinking?
- What is Risk?
- What is a simple Risk Tool?
- How does it integrate into the Process Approach?
- How do you make Risk Based Thinking a Continual Process Improvement activity?

# ISO 9001:2015 Risk & Opportunities

## 4.4 Quality management system and its processes

The organization shall establish, implement, maintain and continually improve a quality management system, including the processes needed and their interactions, in accordance with the requirements of this International Standard.

The organization shall determine the processes needed for the quality management system and their application throughout the organization and shall determine:

f) the risks and opportunities in accordance with the requirements of 6.1, and plan and implement the appropriate actions to address them;

# ISO 9001:2015 Risk & Opportunities

6 Planning for the quality management system

6.1 Actions to address risks and opportunities

6.1.1 When planning for the quality management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) give assurance that the quality management system can achieve its intended result(s);

b) prevent, or reduce, undesired effects;

c) achieve continual improvement.

# ISO 9001:2015 Risk & Opportunities

6.1.2 The organization shall plan:

a) actions to address these risks and opportunities;

b) how to:

1) integrate and implement the actions into its quality management system processes (see 4.4);

2) evaluate the effectiveness of these actions.

Actions taken to address risks and opportunities shall be proportionate to the potential impact on the conformity of products and services.

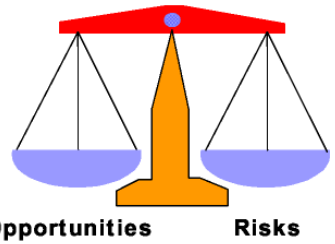
# The Main Objectives of International Standards

- To provide confidence in the organizationôs ability to consistently provide customers with conforming goods and services
- To enhance customer satisfaction

The concept of ñriskò in the context of the international standards relates to the uncertainty in achieving these objectives

# What is Risk Based Thinking?

# What is ñRisk-Based Thinking




- Risk-based thinking is something we all do automatically and often sub-consciously
- The concept of risk has always been implicit in ISO 9001 ï the 2015 revision makes it more explicit and builds it into the whole management system
- Risk-based thinking is already part of the *process approach*
- Risk-based thinking makes *preventive action* part of the routine

- *Risk is often thought of only in the negative sense. Risk-based thinking can also help to identify opportunities. This can be considered to be the positive side of risk*

# Why Should I adopt ñRisk-Based Thinkingò?

- To improve customer confidence and satisfaction
- To assure consistency of quality of goods and services
- To establish a proactive culture of prevention and improvement
- Successful companies intuitively take a risk-based approach

# What Should I Do?

Identify what the risks and opportunities are in <u>your</u> organization ï it depends on context

- ï ISO 9001:2015 will not automatically require you to carry out a full, formal risk assessment, or to maintain a ñrisk registerò
- ï ISO 31000 (ñRisk management ð Principles and guidelinesò) will be a useful reference (but not mandated)

# What Should I Do? (continued)

- Analyse and prioritize the risks and opportunities in your organization
  - *what is acceptable?*
  - *what is unacceptable?*
- Plan actions to address the risks
  - *how can I avoid or eliminate the risk?*
  - *how can I mitigate the risk?*
- Implement the plan – *take action*
- Check the effectiveness of the actions – *does it work?*
- Learn from experience – *continual improvement*

# Key Points to Remember

Risk Based Thinking = Preventative Action

Risk Based Thinking is everybody's business!

- Risk Based Thinking is not just the responsibility of management
- Risk Based Thinking must become an integral part of the organizational culture

# What is Risk?

Risk is the possibility of events or activities impeding the achievement of an organization's strategic and operational objectives.

# Risk ï A Simple Definition

The volatility of potential outcomes.

or

How surprised do you really want to be??

# Food for Thought

## Å Why is Risk like Swiss Cheese?

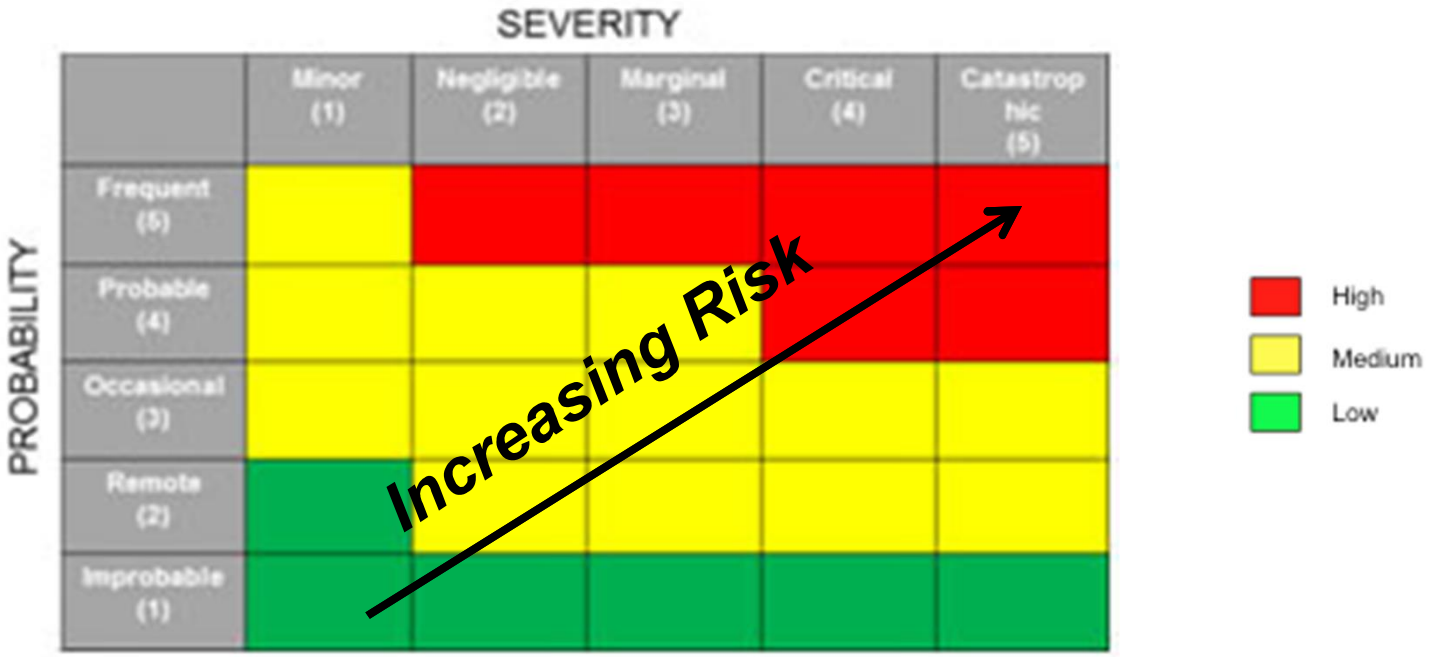

Author needs to acknowledge that this idea was shown at the NQA Meeting, Boston Session, August 2014

# Risk Definitions

Risk can be defined by two (2) parameters

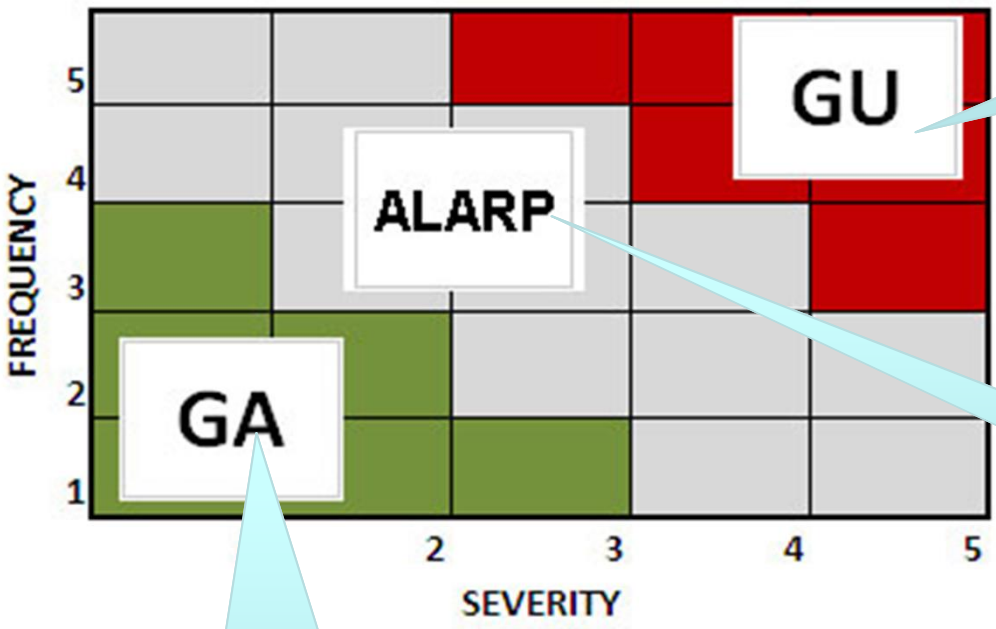
- Severity
  - This is the *Seriousness* of the harm
- Probability
  - This is the *Probability* that the harm will occur

# Risk Assessment - Quantitative




| Severity of Harm | | Probability of Occurrence | |
|---|---|---|---|
| S-5 | Catastrophic | O-5 | Frequent |
| S-4 | Critical | O-4 | Probable |
| S-3 | Serious | O-3 | Occasional |
| S-2 | Minor | O-2 | Remote |
| S-1 | Negligible | O-1 | Improbable |

# Risk Acceptable Regions

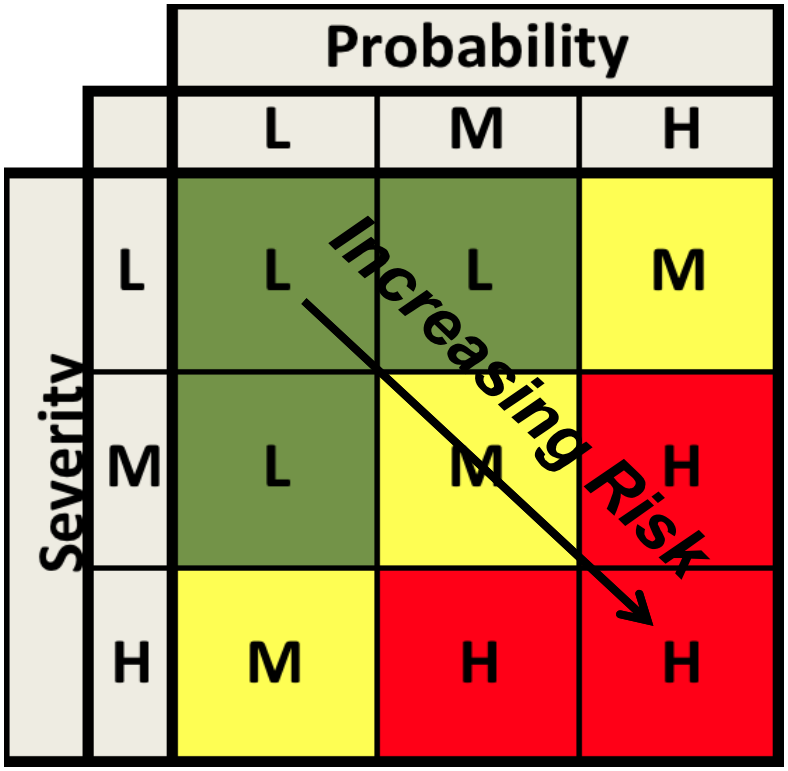



Generally Un-Acceptable

As Low As ñReasonablyò Practical

Generally Acceptable

# Risk Assessment - Qualitative



# Risk Registers

# The Importance of a Risk Register

- The risk register or risk log becomes essential as it records identified risks, their severity, and the actions steps to be taken.
- It can be a simple document, spreadsheet, or a database system, but the most effective format is a table.
- A table presents a great deal of information in just a few pages.

# Components of a Risk Register

There is no standard list of components that should be included in the risk register. Some of the most widely used components are:

- **Dates**: As the register is a living document, it is important to record the date that risks are identified or modified. Optional dates to include are the target and completion dates.
- **Description of the Risk:** A phrase that describes the risk.
- **Risk Type (business, project, stage)**: Classification of the risk: Business risks relate to delivery of achieved benefit;, project risks relate to the management of the project such as timeframes and resources, and stage risks are risks associated with a specific stage of the plan.
- **Likelihood of Occurrence**: Provides an assessment on how likely it is that this risk will occur. Examples are: L-Low >30%)*(, M-Medium (31-70%), H-High (>70%).*
- **Severity of Effect**: Provides an assessment of the impact that the occurrence of this risk would have on the project.

# Components of a Risk Register

There is no standard list of components that should be included in the risk register. Some of the most widely used components are:

- **Countermeasures**: Actions to be taken to prevent, reduce, or transfer the risk. This may include production of contingency plans.
- **Owner**: The individual responsible for ensuring that risks are appropriately engaged with countermeasures undertaken.
- **Status**: Indicates whether this is a current risk or if risk can no longer arise and impact the project. Example classifications are: C-current or E-ended.
- Other columns such as quantitative value can also be added if appropriate.

# Risk Registers - Example

**Risk Register**

Project Name:
Project Manager:
Date:

| Risk | Probability | Impact | Exposure | Mitigation | Contingency |
|---|---|---|---|---|---|
| Supplier does meet the delivery deadlines | Medium | High | High | - Supplier is providing weekly interim releases, which we integrate, test, and track.<br>- Supplier deliveries are prioritized, so highest priority items will be received first. | - Higher priority outstanding items will be moved in-house.<br>- Lower priority outstanding items will be descoped.<br>- Progress of supplier's interim deliveries will feed back into the project plan. |
| Customer does not provide timely feedback on interim releases | Low | Medium | Low | - Project manager and account manager are communicating closely with the customer to ensure that they understand the project's dependency on their deliverables.<br>- For each interim release to the customer, we are tracking how quickly they progress through their evaluation. | - If the feedback is not received in a timely manner, further customer requests will be handled in future releases.<br>- Identify other sources for product feedback.<br>- Customer response time will feed back into the project plan. |
| Project is delayed because of insufficient test resources | Medium | Medium | Medium | Project manager is arranging to borrow staff from other project teams. | If no other testers are available, developers will be assigned as coding ramps down. |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Notes:**
Once a risk materializes, it should be moved to your issues tracking list.
A risk is a specific event that could happen at some point in the future, ie:
"Insufficient test resources" is not a risk.
"Project is delayed because of insufficient test resources" is a risk.
Mitigation: What we're doing to avoid the risk.
Contingency: What we'll do if it happens.

Risk exposure is from the following table:

| | | Probability | | |
|---|---|---|---|---|
| | | **L** | **M** | **H** |
| Impact | **L** | L | L | M |
| | **M** | L | M | H |
| | **H** | M | H | H |

# Risk Registers - Example

## RISK LOG

| | | | |
|---|---|---|---|
| **Project:** | Building Services Replacement DLO System | | |
| **Produced By:** | Glenn Tatton revised by Sue McPherson | | |
| **Given To:** | | | |
| **Version:** | 7 | **Date:** | 2/11/09 |

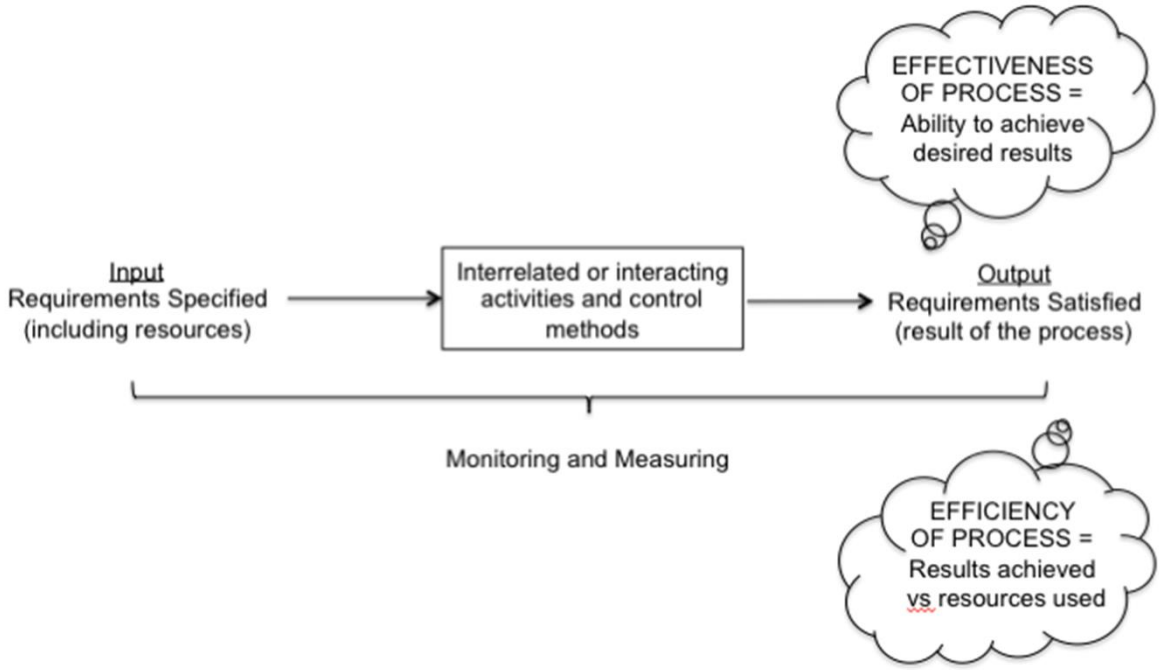
Text in red has been changed since last version. Risks highlighted in grey have been closed.

| No. | Author | Date Raised | Risk Description | Probability (P) | Impact (I) | Risk Factor (PxI) | Proximity | Financial Impact | Managed Response | | | Current status |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | Action | Responsibility | Last Review Date | |
| **Risks in going live:** | | | | | | | | | | | | |
| 1 | GT | 2/7/09 | System may go live with key functionality not working / in place causing major disruption to service. | 4 | 5 | 20 | Now | | Ensure acceptance testing plans include requirements for KNH, D&PS and KD and all acceptance testing is completed before go live. Reps from key stakeholder groups should be involved in the acceptance testing. | PW | 12/10/09 | Open – Outstanding issues on Build. Svcs. issues log: 4 High priority, 1 Medium, 18 with unclassified priority |
| 2 | GT | 2/7/09 | Operatives will not be able to deal with calls from tenants and update the system effectively. | 2 | 5 | 10 | Now | | Ensure all user training is completed before go live. | PW | 14/9/09 | Open – Training of KD & KNH staff in progress. |
| 3 | GT | 2/7/09 | Productivity levels will diminish; staff may reject system as unusable due to unacceptably slow system response times. | 2 ↓ | 5 | 10 ↓ | Now | | Intech to provide physical servers for Total databases and Opti-time live system for Build Svcs to go live on.<br><br>InTech to work closely with third party support companies to identify and resolve system response | Intech | 2/11/09 | Open – New physical server for Total databases has been built. Consilium to build systems on this machine. New physical Opti-time server expected to |

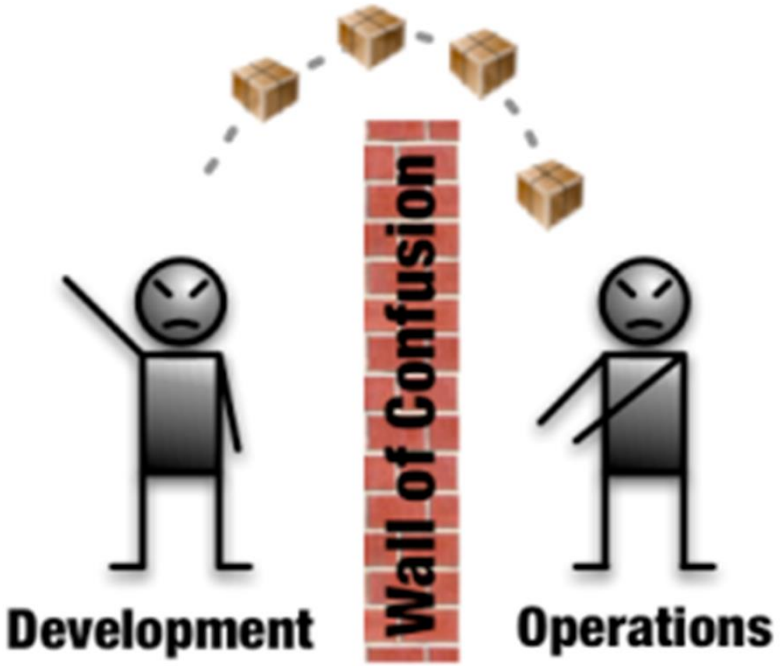
# Integrating Risk Based Thinking with the Process Approach

# Purpose of the Process Approach

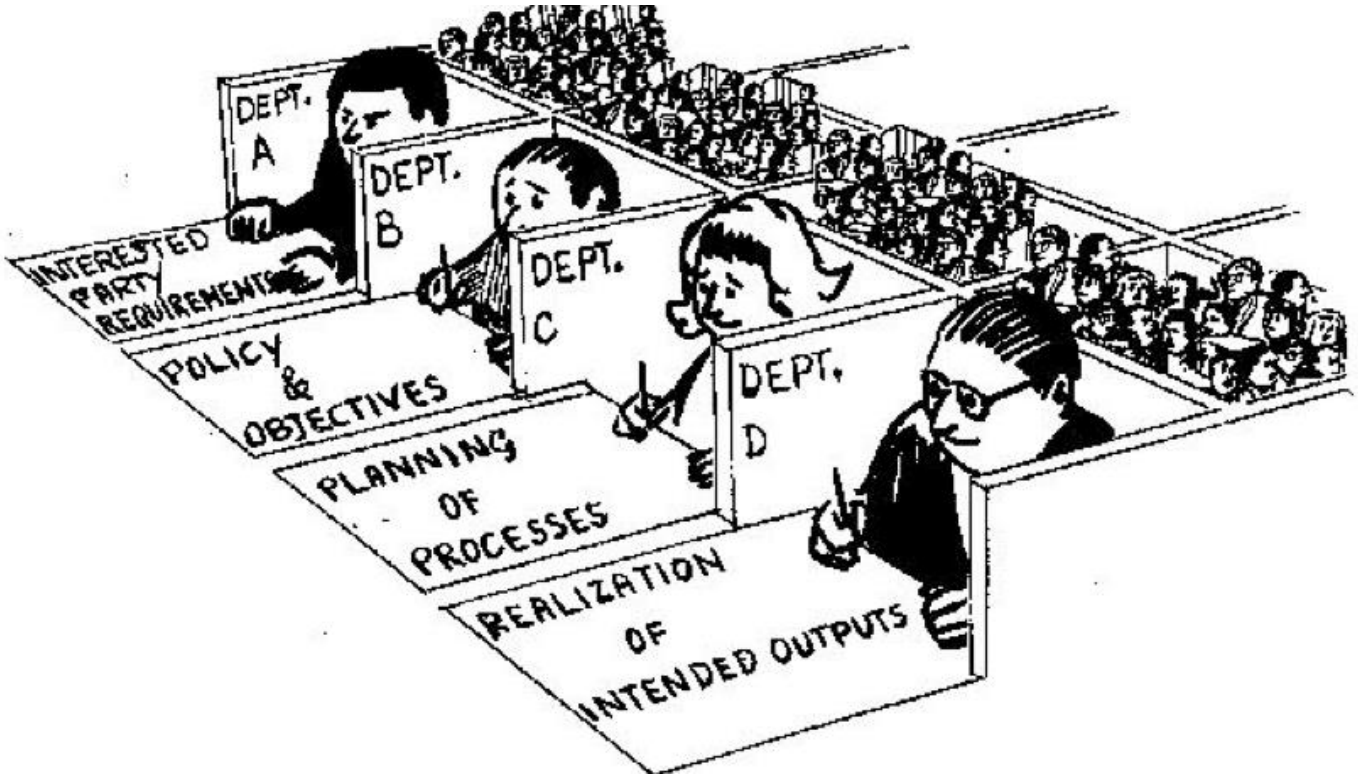
The purpose of the process approach is to enhance an organizationôs effectiveness and efficiency in achieving its defined objectives. This means enhancing customer satisfaction by meeting customer requirements.



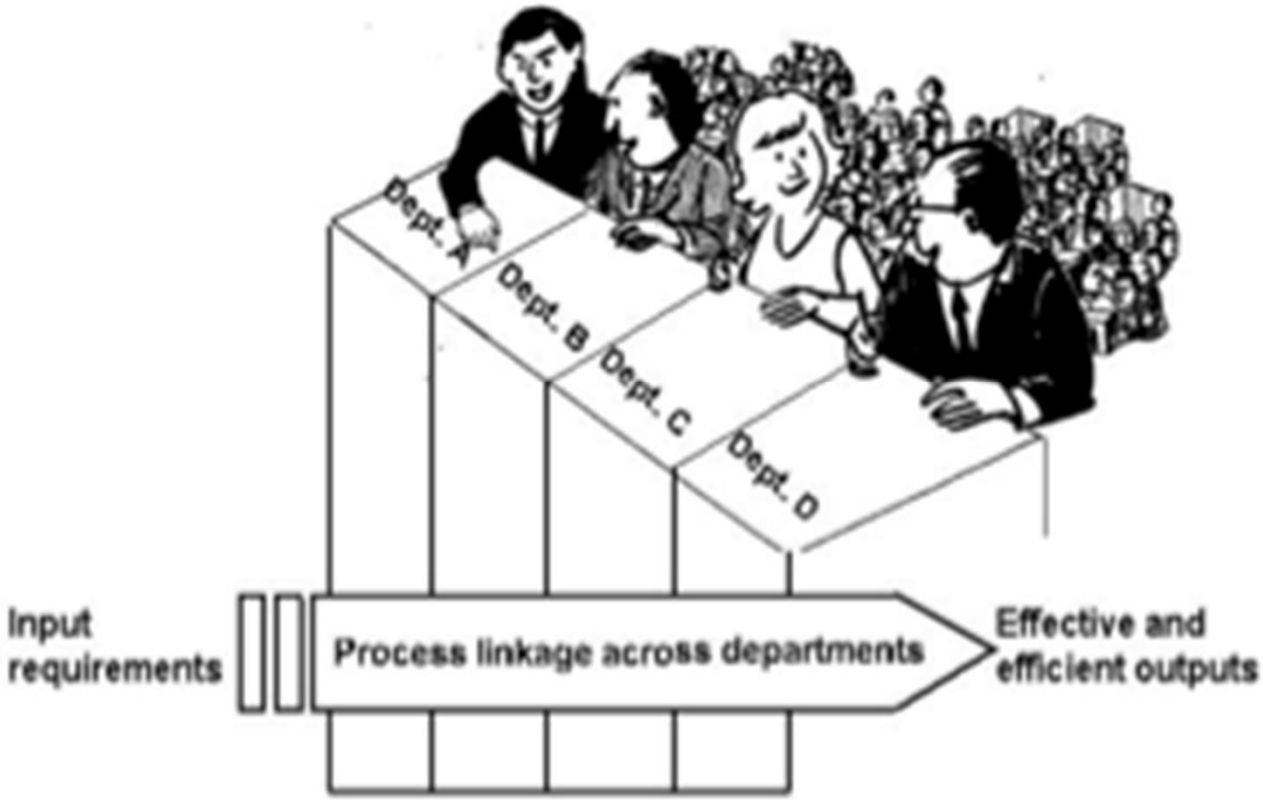
# Is This a Process Model in Your Organization?

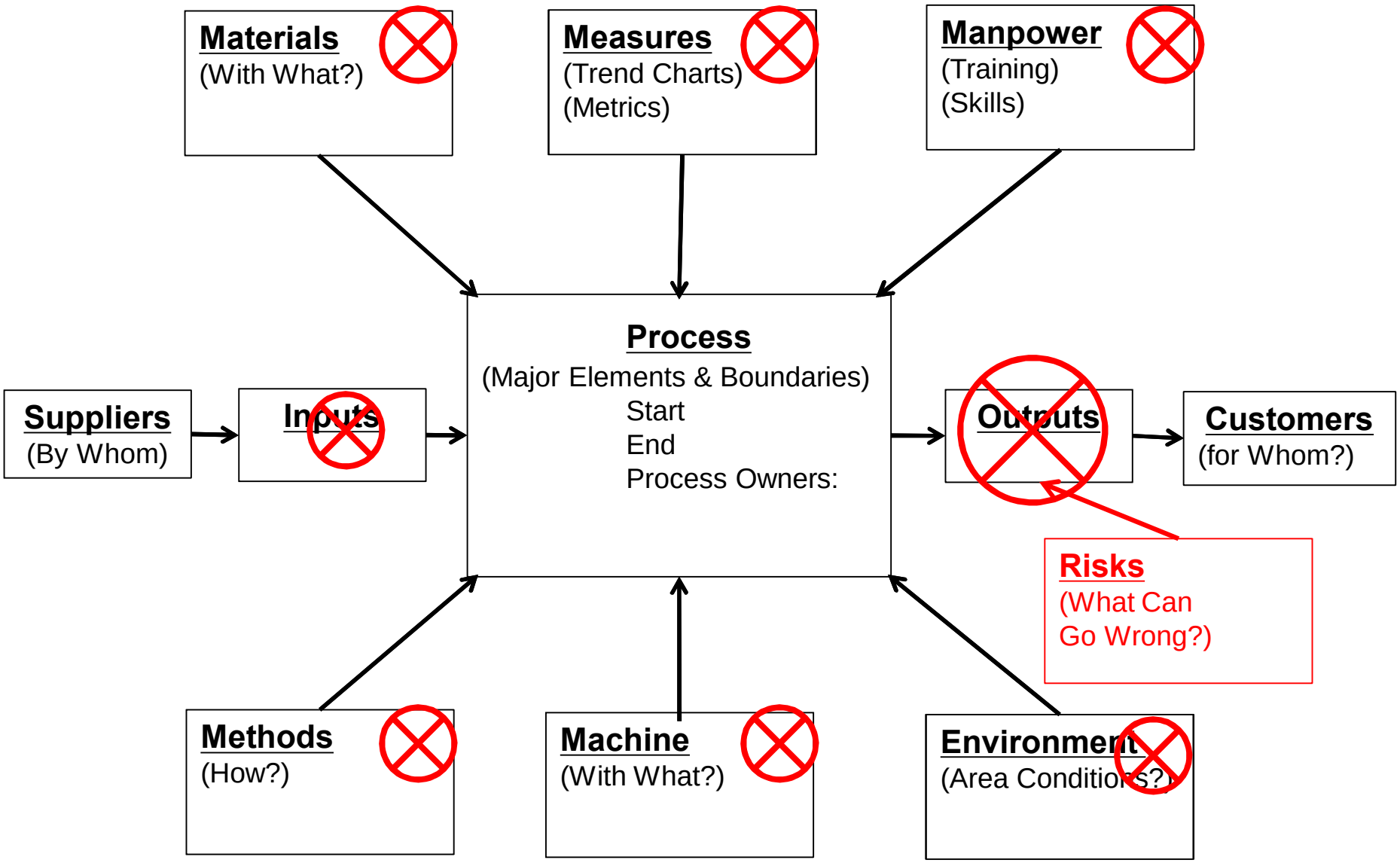


# or does your Process Approach look like this?



# or does your Process Approach look like this?




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?)

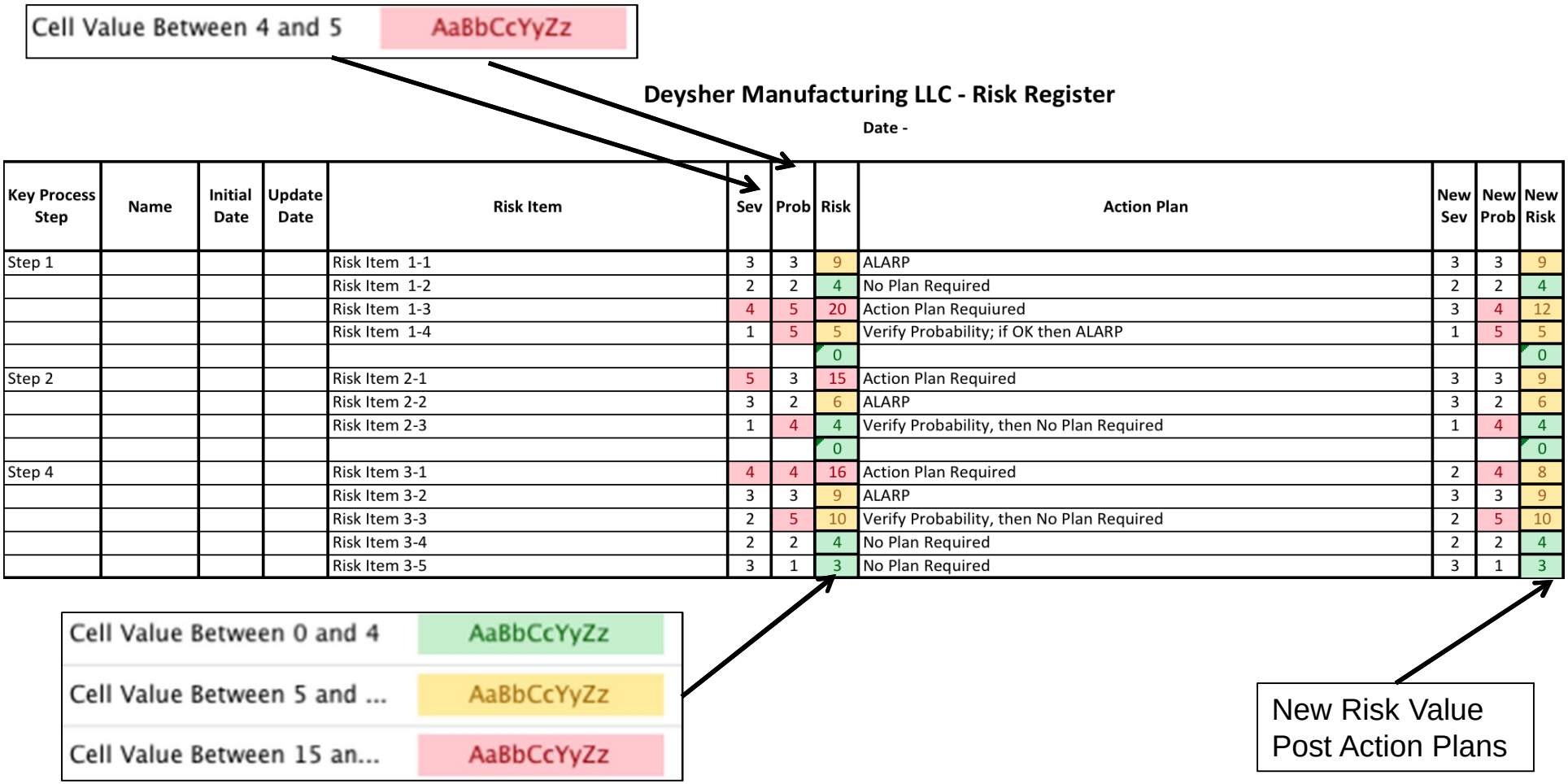
# Proposed Risk Model

**Deysher Manufacturing LLC - Risk Register**

**Date -**

| Key Process Step | Name | Initial Date | Update Date | Risk Item | Sev | Prob | Risk | Action Plan | New Sev | New Prob | New Risk |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Step 1 | | | | Risk Item 1-1 | | | 0 | | | | 0 |
| | | | | Risk Item 1-2 | | | 0 | | | | 0 |
| | | | | Risk Item 1-3 | | | 0 | | | | 0 |
| | | | | Risk Item 1-4 | | | 0 | | | | 0 |
| | | | | | | | 0 | | | | 0 |
| Step 2 | | | | Risk Item 2-1 | | | 0 | | | | 0 |
| | | | | Risk Item 2-2 | | | 0 | | | | 0 |
| | | | | Risk Item 2-3 | | | 0 | | | | 0 |
| | | | | | | | 0 | | | | 0 |
| Step 4 | | | | Risk Item 3-1 | | | 0 | | | | 0 |
| | | | | Risk Item 3-2 | | | 0 | | | | 0 |
| | | | | Risk Item 3-3 | | | 0 | | | | 0 |
| | | | | Risk Item 3-4 | | | 0 | | | | 0 |
| | | | | Risk Item 3-5 | | | 0 | | | | 0 |

# Proposed Risk Model - Populated



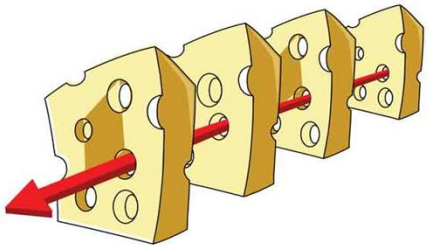

| Key Process Step | Name | Initial Date | Update Date | Risk Item | Sev | Prob | Risk | Action Plan | New Sev | New Prob | New Risk |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Step 1 | | | | Risk Item 1-1 | 3 | 3 | 9 | ALARP | 3 | 3 | 9 |
| | | | | Risk Item 1-2 | 2 | 2 | 4 | No Plan Required | 2 | 2 | 4 |
| | | | | Risk Item 1-3 | 4 | 5 | 20 | Action Plan Requiured | 3 | 4 | 12 |
| | | | | Risk Item 1-4 | 1 | 5 | 5 | Verify Probability; if OK then ALARP | 1 | 5 | 5 |
| | | | | | | | 0 | | | | 0 |
| Step 2 | | | | Risk Item 2-1 | 5 | 3 | 15 | Action Plan Required | 3 | 3 | 9 |
| | | | | Risk Item 2-2 | 3 | 2 | 6 | ALARP | 3 | 2 | 6 |
| | | | | Risk Item 2-3 | 1 | 4 | 4 | Verify Probability, then No Plan Required | 1 | 4 | 4 |
| | | | | | | | 0 | | | | 0 |
| Step 4 | | | | Risk Item 3-1 | 4 | 4 | 16 | Action Plan Required | 2 | 4 | 8 |
| | | | | Risk Item 3-2 | 3 | 3 | 9 | ALARP | 3 | 3 | 9 |
| | | | | Risk Item 3-3 | 2 | 5 | 10 | Verify Probability, then No Plan Required | 2 | 5 | 10 |
| | | | | Risk Item 3-4 | 2 | 2 | 4 | No Plan Required | 2 | 2 | 4 |
| | | | | Risk Item 3-5 | 3 | 1 | 3 | No Plan Required | 3 | 1 | 3 |

# Food for Thought

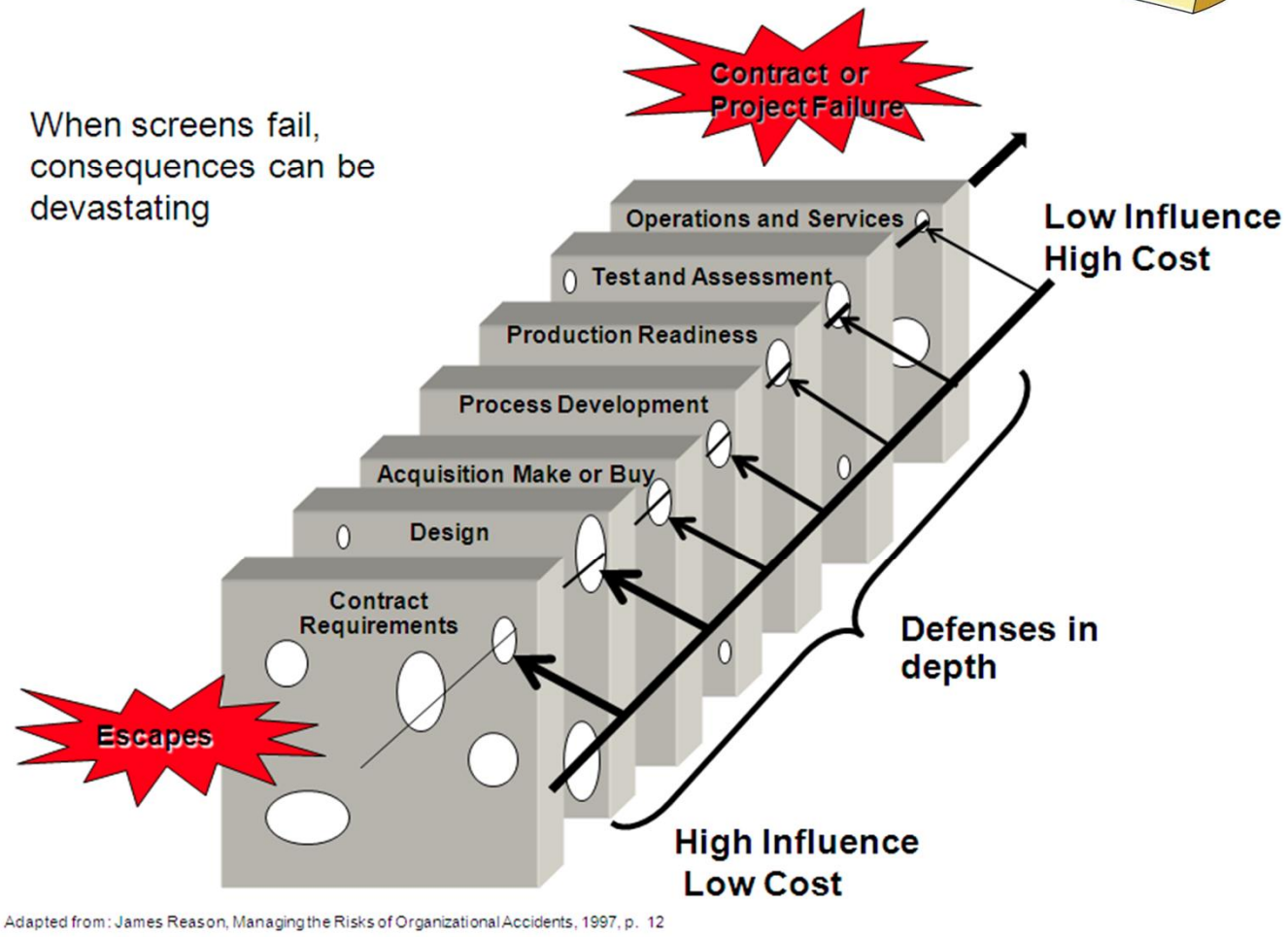
## Å Why is Risk like Swiss Cheese?


Author needs to acknowledge that this idea was shown at the NQA Meeting, Boston Session, August 2014

# Addressing Risk



When screens fail, consequences can be devastating

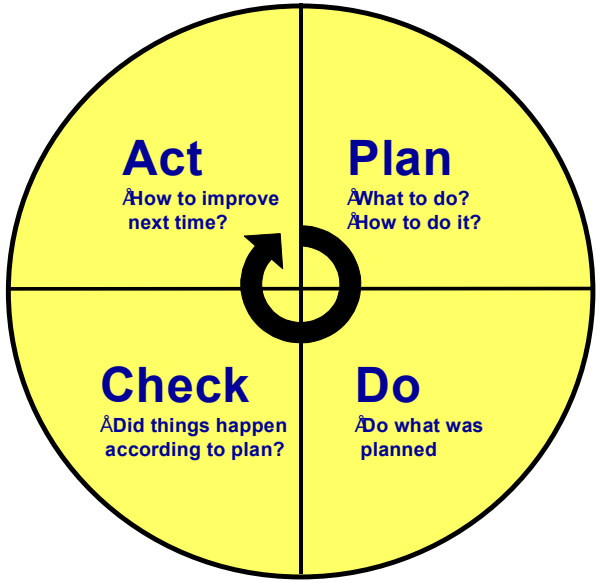



Adapted from: James Reason, Managing the Risks of Organizational Accidents, 1997, p. 12

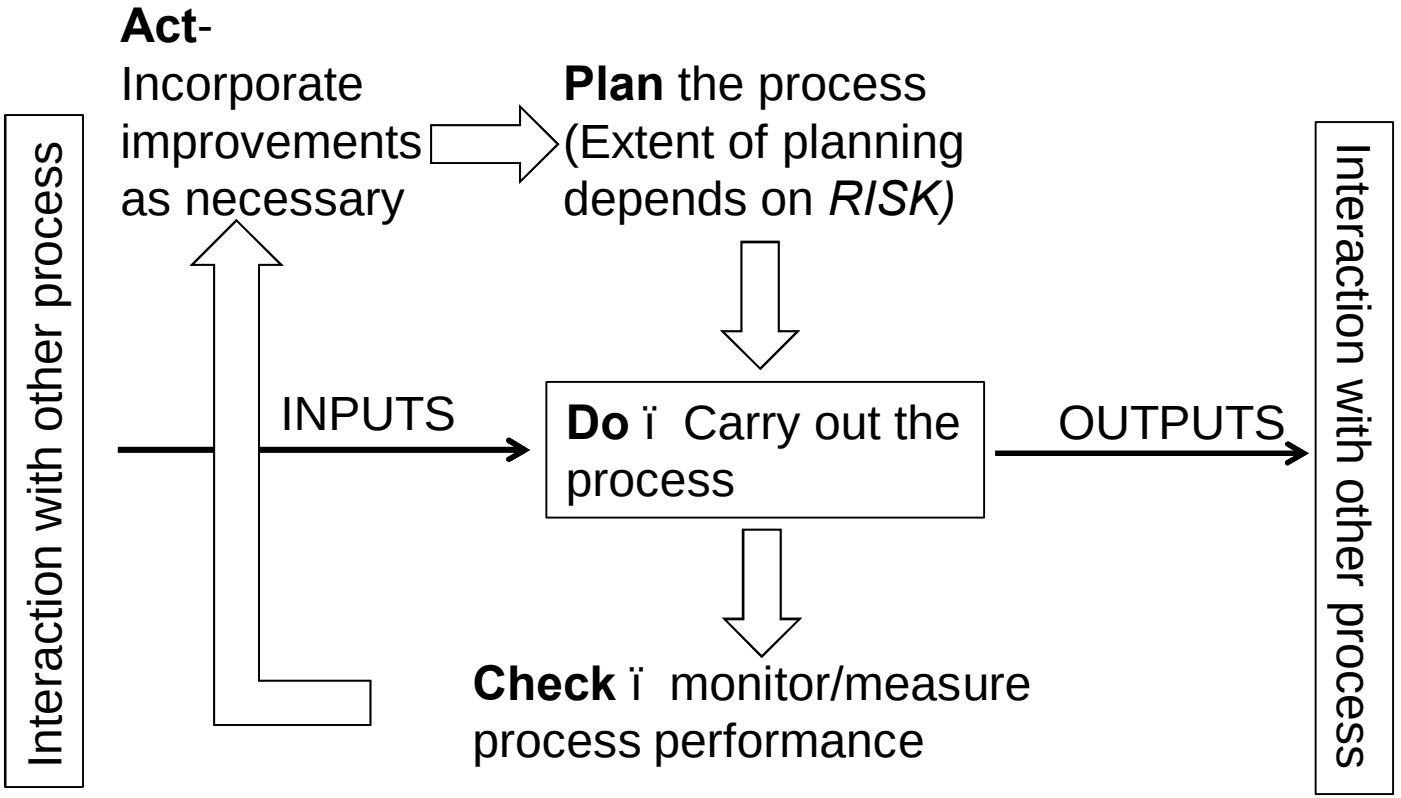
# Integrating Risk Based Thinking with the Process Approach and PDCA

# Plan-Do-Check-Act

The Plan-Do-Check-Act (PDCA) methodology can be a useful tool to define, implement and control corrective actions and improvements. Extensive literature exists about the PDCA cycle in numerous languages



# Process + Risk + PDCA Model




# Management Review Input

Top management shall review the organization's quality management system, at planned intervals, to ensure its continuing suitability, adequacy, and effectiveness.

The management review shall be planned and carried out taking into consideration:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the quality management system including its strategic direction;

c) information on the quality performance, including trends and indicators for:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results;

4) customer satisfaction;

5) issues concerning external providers and other relevant interested parties;

6) adequacy of resources required for maintaining an effective quality management system;

7) process performance and conformity of products and services;

d) the effectiveness of actions taken to address risks and opportunities (see clause 6.1);

e) new potential opportunities for continual improvement.

# Conclusions

- Risk Based Thinking is an element in the Process Approach
- Risk Based Thinking is an input to Management Review
- Risk Based Thinking is an element in the continual improvement process that is focused on prevention.
- Risk Based Thinking has be be demonstrated during audits; a risk register is documented information that validates an organization has done Risk Based Thinking.

# Questions???

# References


- ISO 9000 Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for management systems, ISO/TC 176/SC 2/N 544R3
- ISO 9001:2008
- ISO 9001:2015
- *“Implementing the Process Approach”*, Core Business Solutions, Inc., March 31, 2008.
- The Process Approach: Adding Business Value and Minimizing Risks; David Muil, Intertek.
- The PDCA Continuous Improvement Cycle; Module 6.4; Jeremy Weinstein and Steve Vasovski , 2004