



ERM and SIX Sigma

Auditing within the ERM Framework
using Six Sigma Tools : Merging Two
Philosophies

By Michael Vincent, MBA, CISA, PMP



What is Six Sigma?



Definition

A business driven, repeatable process for quantifying, analyzing, implementing, and sustaining customer-driven strategic, operational, and financial business goals.



Overview

- n **Overall it is a problem solving methodology, that includes :**
 - .. Understanding and Defining Customers
 - .. Understanding and Defining Problems
 - .. Using State of the Art Detective Work Tools (this includes some Applied Statistics) to determine the Root Cause of the Problems
 - .. Proposing solutions based on the detective work data
 - .. Making changes to prevent the root cause from occurring again
 - .. Monitoring the process for further improvements and ever-changing customer requirements

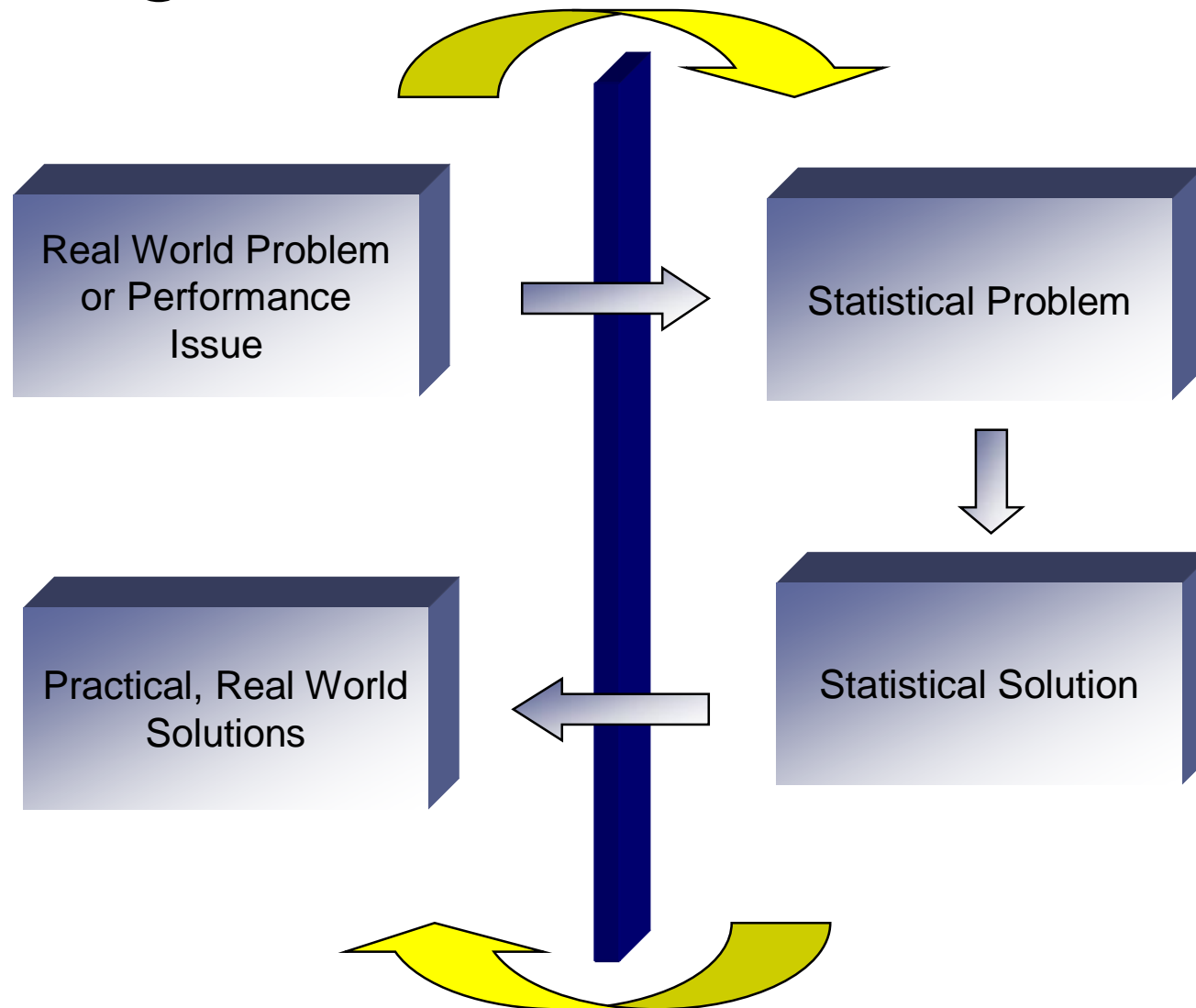
Six Sigma versus Three Sigma Philosophies

The 3 Sigma Company

The 6 Sigma Company

Believes 99% is good and is 99% Good ... 66,807 defects out of a million opportunities	Believes 99% is bad and is 99.9997% Good ... 3.4 defects out of a million opportunities
Relies on inspection	Relies on capable processes
Believes high quality is expensive	Knows high quality means low cost
Defines customer needs internally	Defines customer needs externally
Spends 15% to 25% of revenue dollars on cost of failure	Spends 5% of revenue dollars on cost of failure
Does not have a disciplined approach to gather and analyze data	Uses a structured approach to gather, analyze, and identify improvements through metrics

Six Sigma Flow





The Process



DMAIC

- n Define
- n Measure
- n Analyze
- n Implement
- n Control



DMAIC: Why this structure?

It is a scientific approach to rapid learning that is designed to help prevent a common tendency :

Jumping to Conclusions/Solutions

Some Examples:

- Solutions that do not fix anything (get out the bigger whip)
- Treating the Symptoms (the Whack-a-Mole Game)

2/16/2006 •• The 5 (or more) Whys ... (next slide)

The 5 (or more) 'Whys'

WHY ?

Complaints about Room Service

Cold Food delivered by Room Service

WHY ?

Delivery Process was taking too long

Long Delays Waiting for Service Elevator

WHY ?

Heavier elevator use by housekeeping

Housekeeping was frequently restocking towels

WHY ?

Laundry's washing process was not completed on time

Necessary supplies not available

WHY ?

Vender shipment was late again

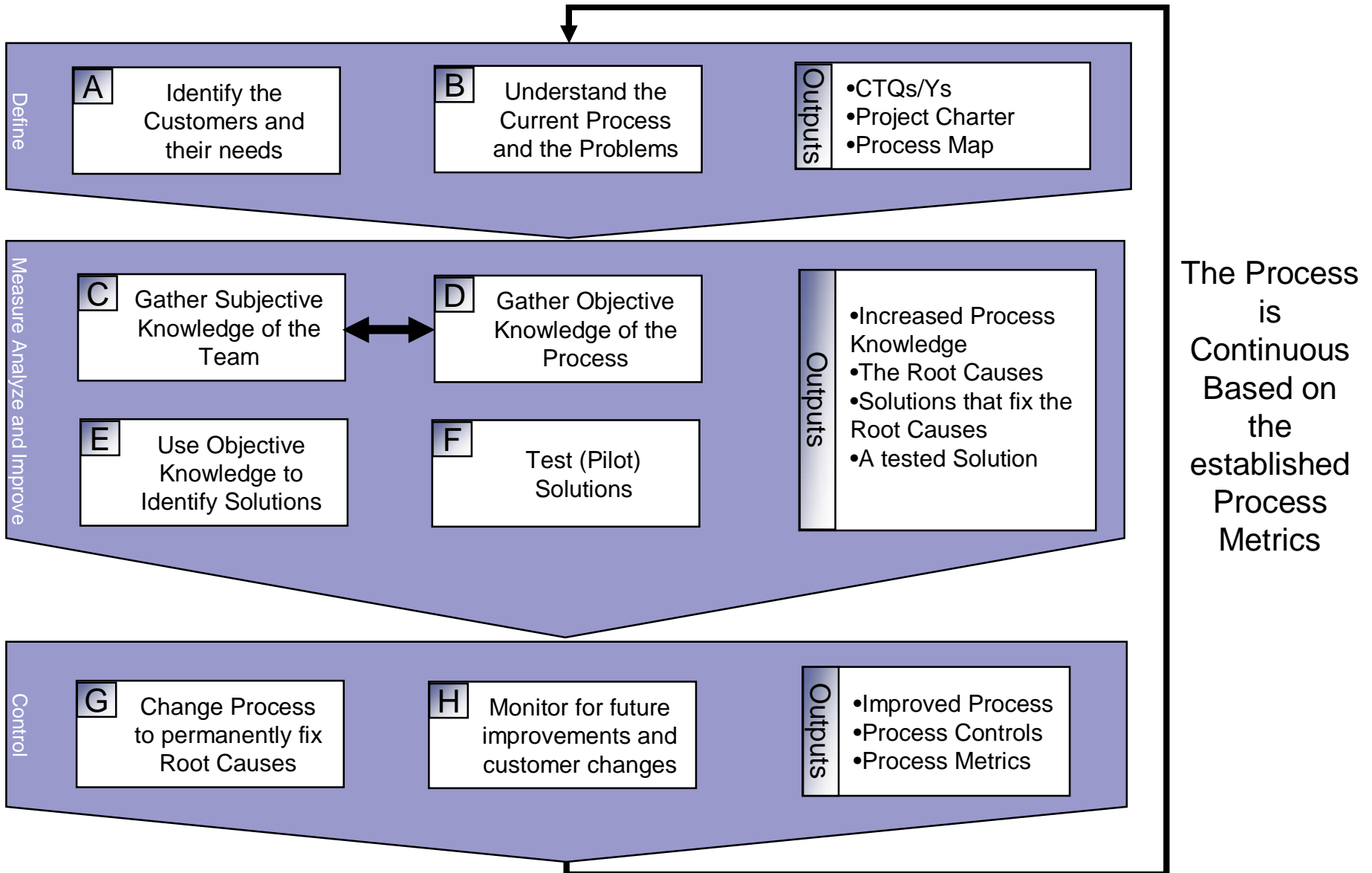
... etc.


WHY ?

WHY ?

WHY ?

The overall structure



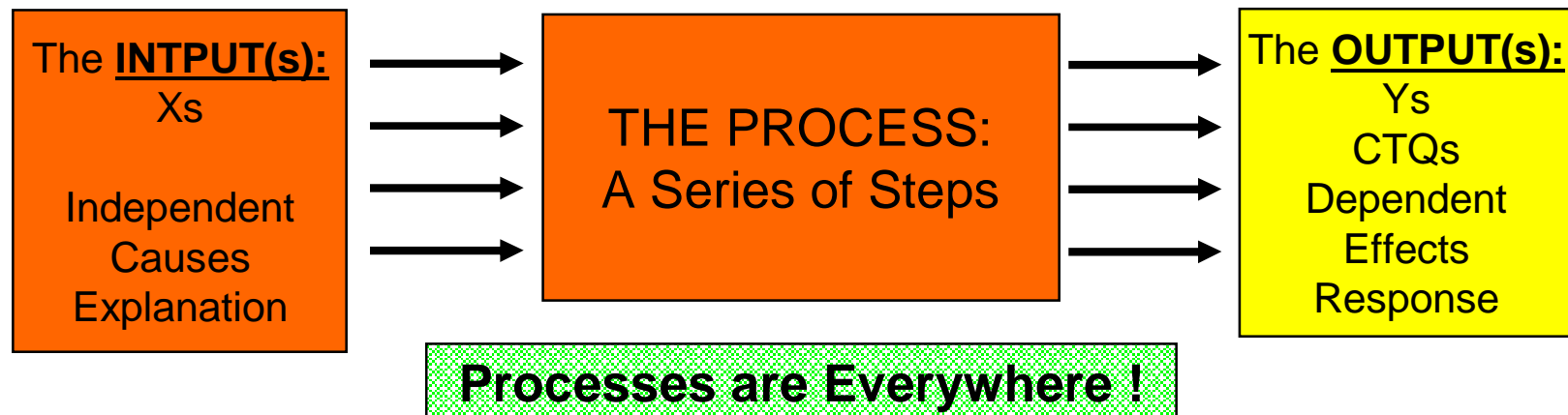


DMAIC - Define

- n Customer
- n Customer Needs
- n Project Team
- n Build Trust
- n Scope

Understand the Current Process

- n Definition of **Process** :
a series of actions or operations conducing to an end
- n When applying to Six Sigma :
The OUTPUT(s) of a PROCESS is a function of the INPUT(s)
$$Y = f(X_1, X_2, X_3, X_4, \dots)$$

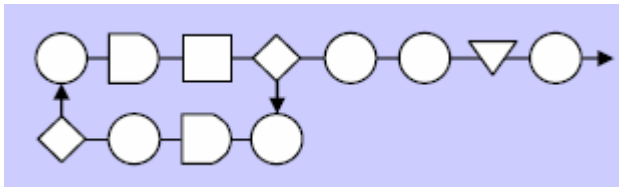


Document the Current Process

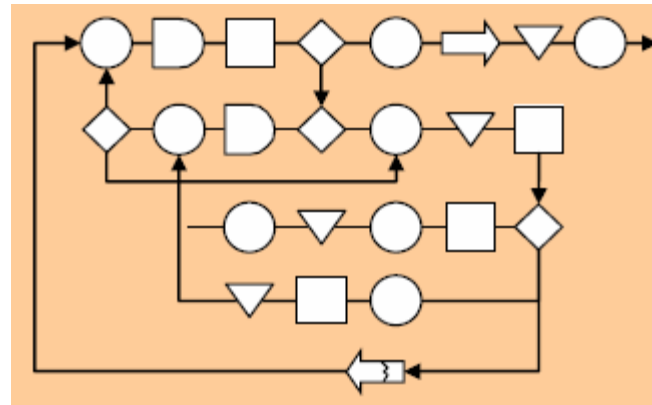
Process mapping is a graphical representation of all process steps

There are always 3 versions :

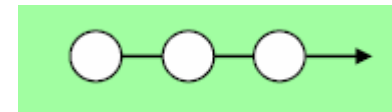
What you THINK it is



What it ACTUALLY is



What you WANT it to be



B Understand the Current Process and the Problems

DMAIC - Measure

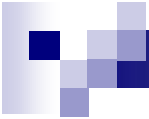
- n Identify metrics
- n Develop precision requirements
- n Identify success criteria of process
- n Identify tools
- n Data, Data, and more data



DMAIC - Analyze

- n Identify and correlate statistically significant potential causation
- n Intense statistical deducing
- n Avoid influencing process while observing
- n Determine 'Correlation' of processes





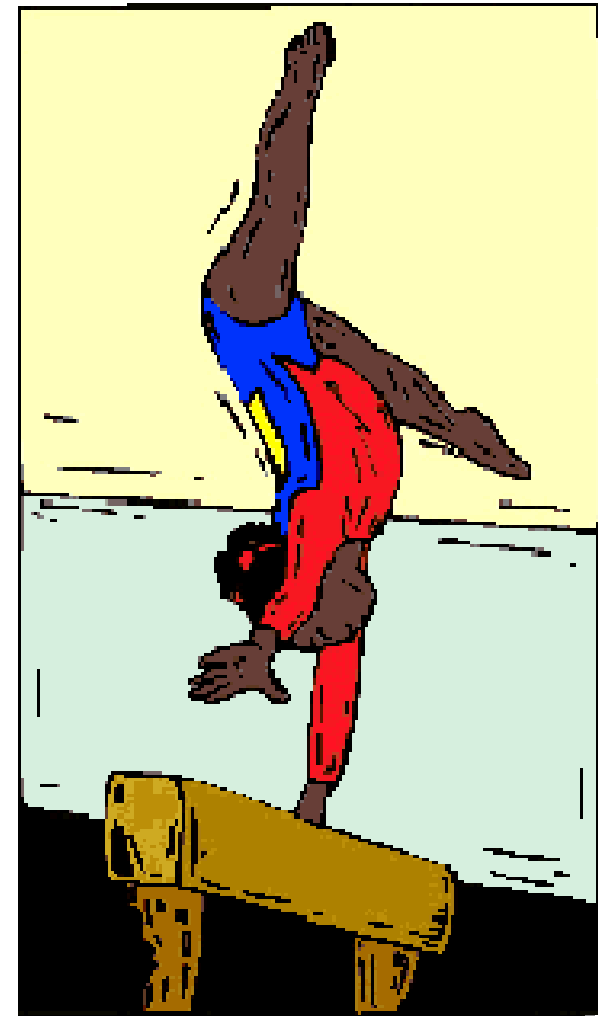
DMAIC - Improve

- n Confirm causal relationship is statistically significant
- n Identify factors that significantly influence process towards customer driven success expectations.
- n Verify that calibrations made to factors significantly influence process towards customer driven success factors
- n Maximize calibrations to their most efficient and effective levels based on customer driven success factors

New and Improved!

DMAIC - Control

- n Identify controls that will maintain calibrations at their desired levels
- n Develop monitoring process for controls
- n Develop fault-tolerances and response mechanisms
- n Document the process
- n Develop continual process improvement methodology
- n Develop a feedback mechanism





What is ERM?

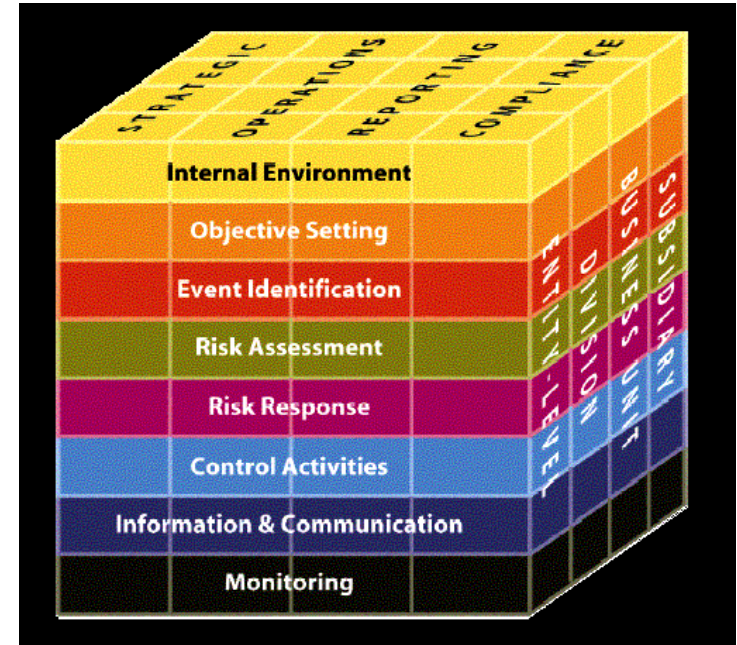


Definition

‘Enterprise risk management is a process, effected by an entity’s board of directors, management, and other personnel, applied in a strategy setting and across the enterprise, designed to identify events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of the entity objectives.’ – COSO Definition

ERM Framework

- n Internal Environment
- n Objective Setting
- n Event Identification
- n Risk Assessment
- n Risk Response
- n Control Activities
- n Information and Communication
- n Monitoring





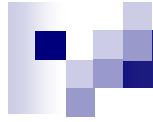
ERM must link to Enterprise Objectives

- n Organizational Objectives
- n Organizational Strategies
- n Organizational Metrics
- n Functional Objectives
- n Functional Strategies
- n Functional Processes
- n Functional Metrics



ERM: Still In Infancy

- n Current Status: ERM is still in infancy with regard to practical application
- n Reason: Difficult to ascertain metrics required to develop risk profile at enterprise level
 - COSO 1 Implementation is in silos and generally only in limited financial risks
- n Unknown-Unknown: Risk Appetite of Organizations
- n Missing Link for Auditors: How to Gather this Information



Hey... You got ERM in my Six Sigma!



Proposal: Quality Methodology Metrics can be input into ERM

- n Where to Begin
- n Gathering the Information
- n Storing the Data
- n Risk Assessment
- n Issue Management
- n Continuous Monitoring : Information and Communication
- n Reaping Results



Proposal: Quality Methodology Metrics can be input into ERM

- n **Where to Begin**
- n Gathering the Information
- n Storing the Data
- n Risk Assessment
- n Issue Management
- n Continuous Monitoring : Information and Communication
- n Reaping Results



Where to Begin

- n Note: This Process requires support of senior management.
- n Develop Program
 - .. Assign Program Manager
 - .. Build Project Plan
 - .. Build WBS
- n Identify Mission of Organization
- n Identify Strategies to Achieve this Mission
- n Identify Objectives/Functions that exist to achieve these strategies
 - .. How are these measured?
 - .. Metrics Objective/Subjective?
 - .. Which functional groups) are responsible?
 - .. What are strategic requirements of IT?
- n Goal: Inventory of Processes and Metrics (KPIs) at Enterprise Level
 - .. Enterprise CTQs
 - .. Operational/Financial CTQs
 - .. IT CTQs
- n Identify ownership of CTQs within organization



Proposal: Quality Methodology Metrics can be input into ERM

- n Where to Begin
- n **Gathering the Information**
- n Storing the Data
- n Risk Assessment
- n Issue Management
- n Continuous Monitoring : Information and Communication
- n Reaping Results



Gathering Information

- n Identify process owners
- n Conduct CSAs
- n Perform “Define” phase of Six Sigma with each process area to refine process maps and critical metrics
 - .. Gather process area metrics
 - .. Gather process area process maps
 - .. Gather process area narratives
- n Define Key Controls within each process/sub-process that support process area CTQ
- n Identify measurement activities using “Measure” phase of Six Sigma
- n Validate that Measurements are accurate and relevant with ‘Analyze’ phase of Six Sigma
- n Purpose: Validating that Metrics being used to support CTQs are complete, accurate, and valid
- n Note: IT must also have metrics (ITIL, COBIT, etc.)
- n Items that cannot be clearly identified are written up as issues



Proposal: Quality Methodology Metrics can be input into ERM

- n Where to Begin
- n Gathering the Information
- n **Storing the Data**
- n Risk Assessment
- n Issue Management
- n Continuous Monitoring : Information and Communication
- n Reaping Results



Storing the Data

- n Store all gathered information in a centralized location
- n ERM Software is abundant
- n Statistical Software (ex. MiniTab, ACL, etc.) can be used to analyze the stored Data
- n Goal: Identify and procure (build/buy) ERM software that fits framework



Proposal: Quality Methodology Metrics can be input into ERM

- n Where to Begin
- n Gathering the Information
- n Storing the Data
- n **Risk Assessment**
- n Issue Management
- n Continuous Monitoring : Information and Communication
- n Reaping Results



Risk Assessment

n Using Inventory of CTQs

- .. Work with process owners, senior management:
 - n Categorize risks
 - .. Inherent, Residual, External, Internal, etc.
 - n Determine likelihood and impact of each risk
 - .. May require both qualitative and quantitative analysis
 - n Identify Risk Response
 - n Validate that controls are in place that mitigate risk
 - .. Identify Issues throughout this process



Proposal: Quality Methodology Metrics can be input into ERM

- n Where to Begin
- n Gathering the Information
- n Storing the Data
- n Risk Assessment
- n **Issue Management**
- n Continuous Monitoring : Information and Communication
- n Reaping Results



Issue Management

- n For CTQs that are not mitigated, measured, or defined appropriately
 - .. Working with management, define issue clearly with language that links to CTQ
 - .. Each Issue is then developed by management as project to develop
 - .. Revisit ERM Model once issue has been mitigated by management
 - .. Issue mitigation technique requires 'Implement' phase of Six Sigma



Proposal: Quality Methodology Metrics can be input into ERM

- n Where to Begin
- n Gathering the Information
- n Storing the Data
- n Risk Assessment
- n Issue Management
- n **Continuous Monitoring : Information and Communication**
- n Reaping Results



Continuous Monitoring: Information and Communication

- n Using CTQ/KPI metrics at multiple levels of organization
- n Build Dashboard of multi-tiered CTQs using an ERM “data warehouse”
 - .. Data mining
 - .. Heat maps
 - .. Exception Reporting
 - .. Executive dashboards
- n This stage is developed and monitored using ‘Control’ phase of Six Sigma



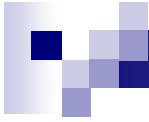
Proposal: Quality Methodology Metrics can be input into ERM

- n Where to Begin
- n Gathering the Information
- n Storing the Data
- n Risk Assessment
- n Issue Management
- n Continuous Monitoring : Information and Communication
- n **Reaping Results**



Reaping the Results

- n Fully Implemented ERM methodology using Six Sigma techniques can:
 - .. Clearly identify CTQs that feed enterprise KPIs
 - .. Translate complex data into actionable information
 - .. Develop predictive modeling infrastructure to anticipate and mitigate risks
 - .. Provide a competitive advantage
 - .. Provide Compliance Infrastructure for Risk Based Audits, Compliance Audits, etc.
 - .. Validate inter/intra process relationships and linkage to organizational objectives
 - .. Enterprise Process Improvement
 - .. Raise awareness of risks to organizational objectives
 - .. Direct correlation of risks to shareholder value
 - .. Quantify enterprise risk appetite
 - .. Assist in providing monetary metrics to CBA exercises (opportunity cost)



Questions?