CONGRESO NACIONAL DE EXCELENCIA EMPRESARIAL 2023

Evolucionando para fabricar un futuro sostenible y competitivo

# *The Intersection of Continuous Improvement and Risk Management*

Mike Nichols, November 23, 2023

# The Role of Continuous Improvement

- Assessment:
  - Identifying improvement opportunities
  - Assessing process maturity
- Improvement:
  - Leading organizational improvement projects
  - Developing internal resources to drive continuous improvement
- Management:
  - Define and report process performance measures
  - Establishing continuous improvement goals
  - Prioritizing opportunities & resources

*Definition of a QMS*:*
*A* formalized system that documents processes, procedures, & responsibilities for achieving quality policies and objectives.

# The Role of Risk Management

- Deployment:
  - Defining risk categories
  - Developing capabilities
- Assessment:
  - Measure & evaluate risk
- Treatment:
  - Mitigate or manage risk
- Manage:
  - Recording, reporting & measuring effectiveness

*ISO 31000:2018 risk categories*:*

Financial
Operational
Strategic

# The Role of Continuous Improvement

- Assessment:
  - Identifying improvement opportunities
  - Assessing process maturity
- Improvement:
  - Leading organizational improvement projects
  - Developing internal resources to drive continuous improvement
- Management:
  - Define and report process performance measures
  - Establishing continuous improvement goals
  - Prioritizing opportunities & resources

*Definition of a QMS*:*
*A* formalized system that documents processes, procedures, & responsibilities for achieving quality policies and objectives.

# The Role of Risk Management

- Deployment:
  - Defining risk categories
  - Developing capabilities
- Assessment:
  - Measure & evaluate risk
- Treatment:
  - Mitigate or manage risk
- Manage:
  - Recording, reporting & measuring effectiveness

*ISO 31000:2018 risk categories*:*

Financial
Operational
Strategic

# Comparing ERM & ECI

## ERM

- Process Mapping
- Key Risk indicators
- Maturity assessments
- Audit reviews
- Periodic review of controls
- Building RM capabilities

## ECI

- Process Mapping
- Key Process indicators
- Maturity assessments
- Root Cause analysis
- Voice of the customer
- Building CI capabilities

These are only a few of the many tools that both disciplines use.

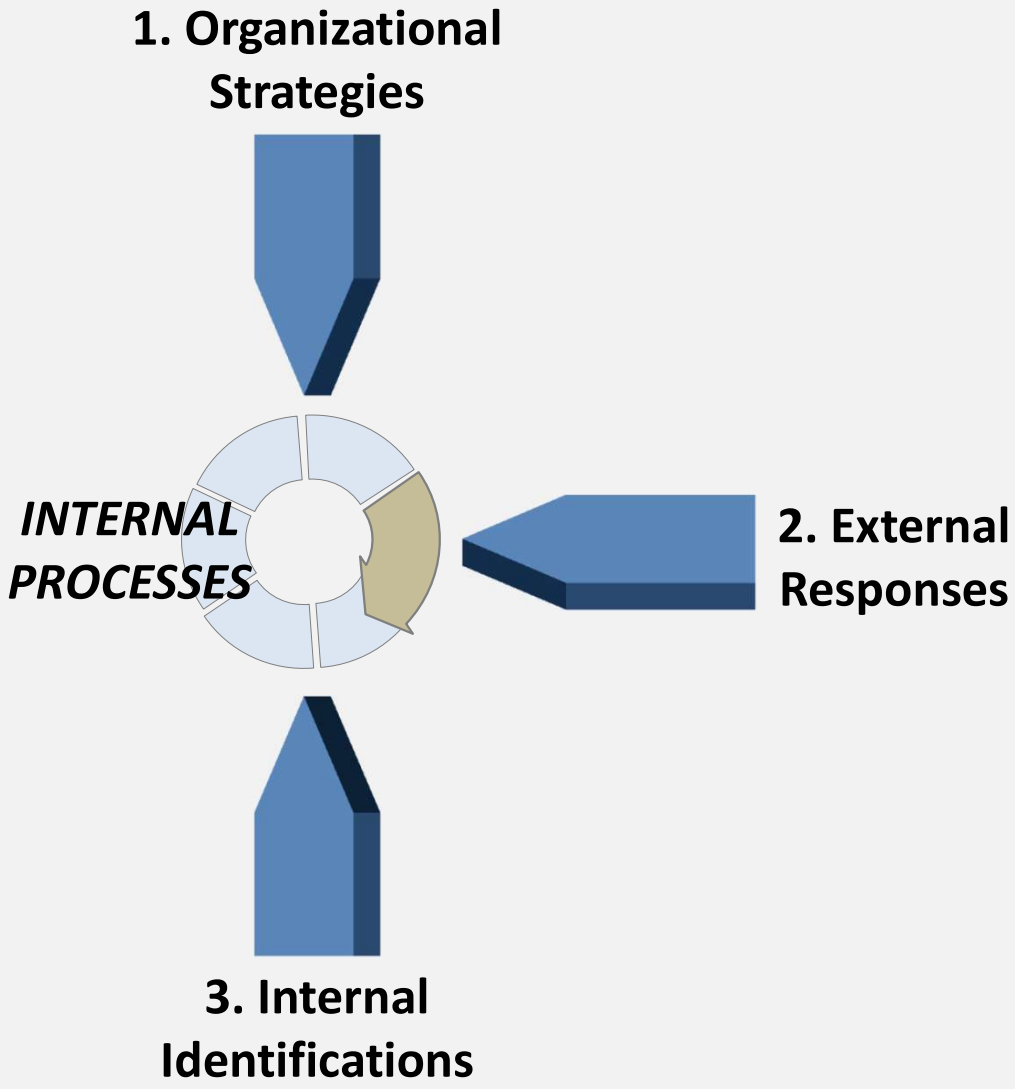
# Where does ISO 31000:2018 fit?

## ISO establishes principles for ERM such as:

- Risk should be integrated into decision making.
- Should have a structured framework with assigned roles and responsibilities.
- Continual improvement of the risk management processes to insure continuous risk identification and treatment.

# Insights For Partnership

*Each of these categories are used to organize the insights shown on the following slides.*



# Organizational Strategies – Group 1

a. Goal alignment & ownership.
b. Role & responsibility clarification.
c. Integrated & shared reporting.
d. Planned cross functional resource support.
e. Designed feedback mechanism from group 3.

# External Responses – Group 2

a. Regulatory requirements
   - Accounting restatements,
   - Loss reporting, or
   - Incident data collection

b. Industry benchmarking

c. Scenario assessment techniques

# Internal Identifications – Group 3

a. Creating a culture of change
b. Align on risk categories
c. Cross functional training
d. Process reviews from two views
   - Risk assessment & FMEA
   - Timely communication of …
e. Joint ownership of some KPIs & KRIs

# What About Here in Costa Rica?

We sent out a survey (55 responses):

- 89% stated the company the work with have a Continuous Improvement department or program.
- 64% stated the company the work with have an Enterprise Risk Management department or program.
- 54% saw evidence of the two groups working together.
  Some examples of what was shared:
  - *Providing joint training.*
  - *Identifying potential measures.*
  - *Sharing potential improvement opportunities and potential risks between groups.*

# Questions?


**Thank you for the opportunity to enjoy your wonderful country and your hospitality!**

# KPI & KRI definitions

- **KPI** – A Key Performance Indicator measures performance or target achievement, often against a customer's requirements. *Example: Production Cycle time for a product.*
- **KRI** – A Key Risk Indicator measures the level of exposure to some operational risk. They could be looking at likelihood of occurrence or potential impact. *Example: Regulatory compliance violations.*
- **KCI** – A Key Control Indicator measures the effectiveness of a control. *Example: Ability to identify when a potential risk has occurred.*

*KCI is a more recent term, not widely used.*

# ISO 31000 Principles

- The principles are foundational in all aspects of risk management and have been incorporated within the sections of this handbook.
- Risk management is integrated: Risk should be considered during normal business activities and decision-making throughout the organization and integrated within the organization's overall management system.
- Risk management arrangements should be structured and comprehensive: A structured framework assists organizational understanding of roles and responsibilities and provides consistent procedures. These include procedures to identify, understand and treat risk and communicate information.
- Risk management is customized: This principle encourages organizations to customize risk management to their organization's objectives and needs.
- Risk management is inclusive: Timely and appropriate engagement of stakeholders enables a wide range of views to be considered as part of risk management, resulting in better-informed decisions.

# ISO 31000 Principles (cont.)

- Risk management is dynamic: As an organization's context and circumstances change over time, so will its risks. This principle reinforces that risks are to be periodically reviewed to ensure that they are addressing organizational objectives.
- Best available information: Informed decision-making requires relevant and accurate information from the organization as well as from other sources. Risk management should reflect and consider the input of internal and external stakeholders.
- Human and cultural factors: Risk management involves collaboration and the engagement of stakeholders. This can result in understanding the human and cultural factors most important to organizational success. This principle also refers to taking unique circumstances and human needs into account when integrating risk management into the organization and developing appropriate risk management processes.
- Continual improvement: This principle encourages an organization to continually monitor, review and improve risk management processes to ensure their relevance, efficiency, and effectiveness in support of the organization's overall performance. Licensed

# Common Operational Risk Categories

- Business disruption,
- Information Security or Cyber risk,
- Operations or Process risk,
- Compliance risk,
- Legal risk,
- Security of Physical Assets,
- Data Management or Data Quality risk,
- Business Model Risk,
- Systems risk,
- Fraud risk,
- People risk (i.e., loss of key personnel, etc.),
- Third Party risk.