INTERNAL CONTROL BASED ON THE COSO REPORT

Objective

- To use **COSO**, the Corporate Governance model, and **COBIT**, the Information Technology Governance framework, to achieve compliance with the SARBANES-OXLEY law
**Scope**

- New paradigms.
- Methodology concepts of COSO.
- MEYCOR COSO AG basics, a tool for implementing internal control based on the COSO report.

**COSO Report**

- In 1992 COSO published *Internal Control—Integrated Framework*, a report that established a common definition of internal control and provided a standard through which organizations could assess and improve their control systems.
The COSO goals

- To improve the quality of financial reporting by focusing on corporate management, ethical standards and internal control.
- To unify the concept of internal control considering the various interpretations and concepts on the matter.

Enterprise Risk Management (ERM)

- Internal control is encompassed within and an integral part of enterprise risk management.
- Enterprise risk management is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk.
- Internal Control—Integrated Framework remains in place for entities and others looking at internal control in itself.
**Basel II**

- Developed several changes that, even if mandatory as of 2007, they set a course where to begin.
- Basel I focused on credit and market risk analysis. Now equity regulation is increasing as demanded by regulatory bodies and risk exposure.
- It now covers the need to consider a new risk: the operational risk, i.e., the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

**Methodology concepts of the COSO Report**

The new Internal Control concepts in organizations
Internal Control definition

- It is a process that involves people at every level of the organization without exceptions, designed to provide a reasonable support to the achievement of objectives in the following categories:
  - Effectiveness and efficiency of operations (O)
  - Reliability of financial reporting (F)
  - Compliance with applicable laws and regulations (C)
- These three categories are interrelated.

What can you get through COSO?

- The definition of a framework that can be applied to any organization.
- COSO considers that internal control should be a process integrated with the business that helps achieving expected results regarding profitability and performance.
- Convey the concept that the effort involves the whole organization: from Senior Management to the newest employee.
Internal Control Components

- 5 components (Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring) that interact with each other and are integrated to the management process.
- The control system should be embedded seamlessly with the operational activities of the organization.
- This helps foster the quality of authority delegation, prevent losses and achieve a fast response to changes.

Control Environment

- Is the basis for the rest of the components, contributing discipline and structure.
- It includes: integrity and ethical values, the entity's employees competence, management's philosophy and operating style, the assignment of authority and responsibility, the organization and development of human resources and the management's direction.
Risk Assessment

- First, consistent organizational goals must be identified and linked. Then the relevant risks that can negatively impact those objectives must be identified and assessed.
- Risks should be managed, considering the changing internal and external environments.

Control Activities

- They are the policies and procedures that help ensure that measures are in place to limit the risks that may impact the organization's objectives.
- E.g., authorizations, verifications, reconciliations, segregation of duties, operational profitability reviews, etc.
**Information and Communication**

- The information required must be identified, captured and communicated in a form and timeframe that enable personnel to carry out their responsibilities.
- The information can be financial or operational, from internal or external sources.
- Appropriate communication channels must exist.
- Personnel must be informed of the importance of their involvement in the effort to apply internal control.

**Monitoring**

- A process must exist to verify that the internal control system continues to function over time.
- This monitoring includes permanent tasks and regular reviews. The frequency of the later will depend on the assessment of the importance of the risks involved.
Interrelationships

- The organization must comply with the three categories mentioned for the objectives (O, F, C).
- The 5 components described are simply the actions necessary to achieve those objectives.

Limitations to be addressed

- The reliance on the internal control system should acknowledge that:
  - Failures may exist as a result of judgment errors.
  - The collusion of two or more people or management’s actions can circumvent the system.
  - The designed system must specify the limitations on resources (cost versus benefit).
Roles and Responsibilities

- Senior Management is ultimately responsible for the control system. Integrity and ethics should be elements that set the example for the rest of the employees. It must direct the managers that are in turn responsible for their corresponding areas.

- The Board of Directors sets the guidelines and the global vision of the business. The Board must have an active role in understanding the actions being performed and it must ensure it has effective communication channels with the Senior Board and the financial, legal and internal audit departments.

- The Internal Audit should monitor the permanency and efficiency of the control systems. In order to do this they must have an adequate hierarchical position.

- The employees at large have the responsibility of participating in the effort of applying internal control, and these details should be included in everyone's job description. All personnel are responsible for communicating upward risks such as problems in operations, non-compliance with the code of conduct, and other policy violations or illegal actions.
The COSO report defines an structure, a framework.
Within this framework we must analyze how components interact for the specific situation of each organization.
A tool must be available to assist in the process of performing regular and proactive assessments of the internal control system.
The assessment can be focused on a single objective (e.g., financial information), or it can involve a specific organization unit or activity.
Risk Assessment

- Establish the objectives.
  - ✓ Global objectives (such as the Mission).
  - ✓ Specific objectives for the different activities (e.g. Production), these sub-objectives must be consistent and measurable by indicators.

The objectives should be:

- Defined in such a way as to identify the criteria used to measure performance and to establish Critical Success Factors (at an activity or operational unit level).
- Consistent and compatible.
- As an example we can consider: to make payments only for authorized purchases, that computer systems should be available according to business requirements, etc.
The risks

- Risk identification and analysis is an interactive process that involves the personnel responsible for achieving the established objectives.
- Risks can be the result of internal and external factors, for instance: breakdowns in computer systems, changes in the responsibilities of the executives, etc.
- Once these risks are identified you must quantify its importance, assess their likelihood to impact the organization and plan the measures to mitigate their effects.

Control Activities

- They are the policies, procedures and actions that affect one or more areas within the organization.
- Some examples are:
  - Analysis performed by management.
  - Direct management by those responsible.
  - The information process.
  - Physical controls.
  - Performance indicators and segregation of duties.
Relationship between elements

- Control activities that adequately address risks help achieve the objectives of an area or an activity, hence achieving the business goals.

Information and Communication

- The quality of the information provided must be ensured; it cannot be just “mere data”.
- Information should be protected since it is a valuable asset.
- Internal communication channels must ensure that all personnel understand enough elements to perform their tasks.
Monitoring

- Includes continuous monitoring and specific assessments.

- Any deficiencies detected must be timely communicated.
Logging into the System

The system controls access using logins and passwords.

The Administrator (ADMIN) should be familiar with the tool and its theoretical framework, and at the review stage he will determine the access to the questionnaires according to the profile of the reviewers.

Main Menu

The main menu includes a toolbar to provide easy access to the most frequently used options.
Workgroups and Reviewers

Here you can define the workgroups and the reviewers that will participate in the review.

Methodology Guide

A methodology guide is available to easily apply the COSO methodology. This guide includes all the steps to be followed during the assessment, together with documentation and shortcuts to the forms where the information is entered.
General Questionnaires

The general questionnaires on the 5 components can be assessed at different organization levels.

General Questionnaires Forms

The general questionnaires can be generated in RTF format (with manual entry of answers) or HTML format (with automated entry of answers).
Load answers from HTML Form

This form allows to load the answers to the general questionnaires from the HTML forms.

Off-line Assessments Synchronization

This form allows to synchronize the answers to the general questionnaires that the reviewers entered in an off-line database.
General Questionnaires Report

Allows to assess the results of the review of the 5 components both graphically and numerically, with different break-down levels.

General Questionnaires Comparison

Allows to compare the review results against themselves and against the average, both graphically and numerically, with different break-down levels.
Comparison between different Periods

Allows to compare the results obtained during different periods, both graphically and numerically, at different breakdown levels.

Organizational Structure Coding

Before beginning the review, you must determine the levels comprised in the organization’s structure.
The organizational chart should be identified, defining the objectives and responsible for each area.
Processes and Sub-processes are defined and assigned to their corresponding units within the organizational chart.

Process and Sub-processes Report
Processes Assignment

You must assign to each workgroup the processes and sub-processes that will be reviewed by them.

Process Weighing

Processes and sub-processes can be weighed and ranked in order to determine which activities are critical for the business and therefore require more attention.
Input Process Activities

Processes and Sub-processes assigned to units.

Hierarchy of the tasks performed in the process.

Risks and Control Activities

It is possible to select the control activities that later on will be audited.

Define the control objectives, the risks and the control activities relative to the processes and sub-processes to be assessed.
Select Control Activities to be Audited

Using filters it is possible to select from all the control activities only those that need to be audited.

Create Audit Projects

Reviewer users can create Audit Projects. For each project you must define the assigned auditors and the process objectives that will be audited.
Assign Objectives and Risks

The reviewer that created the project must define the objectives to be audited by each Auditor. The risks for each objective encompassed by the audit project should also be defined.

Audit Control Activities

Objectives and Risks to be audited according to the Auditor's assignment.

- Record findings
- Link files
- Record tasks performed
Final Audit Report

Selection of observations that are included in the final report.

The final audit report is generated automatically.

Exposure calculation

Impact x Risk Likelihood
Control Activity Assessment

<table>
<thead>
<tr>
<th>CONTROLS AND RISKS MATRIX</th>
<th>CONTROLS</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GOOD</td>
<td>FAIR</td>
<td>BAD</td>
<td></td>
</tr>
<tr>
<td>RISK</td>
<td>4</td>
<td>2.5</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>4.00</td>
<td>6.40</td>
<td>16.00</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>2.50</td>
<td>4.00</td>
<td>10.00</td>
</tr>
<tr>
<td></td>
<td>6.25</td>
<td>1.56</td>
<td>2.50</td>
<td>6.25</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>1.00</td>
<td>1.60</td>
<td>4.00</td>
</tr>
<tr>
<td></td>
<td>2.5</td>
<td>0.63</td>
<td>1.00</td>
<td>2.50</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>0.25</td>
<td>0.40</td>
<td>1.00</td>
</tr>
</tbody>
</table>
# Risks and Control Activities Report

This report assesses the compliance with the control objectives in order to determine if, faced with the identified risks, these are adequately covered.

It is possible to view the risks' weight and the assessment results for existing control activities.

## Allows to assess the results of the objectives review both graphically and numerically.
Risk and Control Activities Summary

Allows to display a summary of the objectives review results and of the processes' risk factors.

Risk Maps and Exposure Charts

Risk Map according to likelihood and impact

Exposure chart considering the assessment of controls.
Risk Treatment

Define the treatment for the different risks.

According to the treatment performed, you can simulate the change in risk exposure.

Define Improvement Projects

The new controls included in the treatment are grouped in implementation projects.

Projects are prioritized according to their impact and cost-risk ratio.
Comparison between different Periods

Allows to compare the processes' assessments obtained during different periods both graphically and numerically.

Meycor COSO Web
Publish, Distribute and Review Documents

The web module included in Meycor COSO AG enables the publication and distribution of documents in a simple yet effective way, being also possible to issue opinions on the documents read.
Meycor COSO Web
Answer General Questionnaires

Meycor COSO web allows to answer the self-assessment questionnaires remotely.

MEYCOR COSO AG includes the following features in order to customize and enhance the detail level of the review:
Includes a methodology guide that eases the application of the COSO methodology and assists you during the entire review process.

Allows to codify the hierarchical levels within the organization in order to determine an organizational chart according to the naming conventions used.

Allows to identify processes and sub-processes, perform a ranking of the same and to link them to their corresponding areas.

Allows to create workgroups and reviewers to facilitate the distribution of tasks.

Allows to assign Administrator privileges to the reviewers.

Includes the objectives, risks and general control activities of the COSO Report.

Allows to manage several versions of the general questionnaires.

Allows to select the control activities that later on will be audited.

Allows to use weighing ratios for processes, objectives and risks.
- Allows to assess the general questionnaires at any hierarchical level.
- Allows to export all the reports in RTF, HTML and EXCEL formats.
- Allows to export all the charts in BMP format.
- Generates general questionnaires assessment forms in HTML format.
- Allows to synchronize general questionnaires and risk and control activities assessments from off-line databases.

- Allows multi-user access to the risks and control activities assessment.
- Allows to create a process ranking.
- Allows to compare results obtained during different periods.
- Includes on-line help.