

By Neil Leigh

This paper takes a look at the practicalities of implementing the COSO 2013 Internal Control Framework with the help of one particular software application. The software in question is Objective Controls, a framework in itself for managing objectives, risks and controls in an integrated and comprehensive manner. COSO and Objective Controls are in my opinion marvelously complementary to each other, each bringing their own unique contribution to the mission of putting internal control management into an organization.

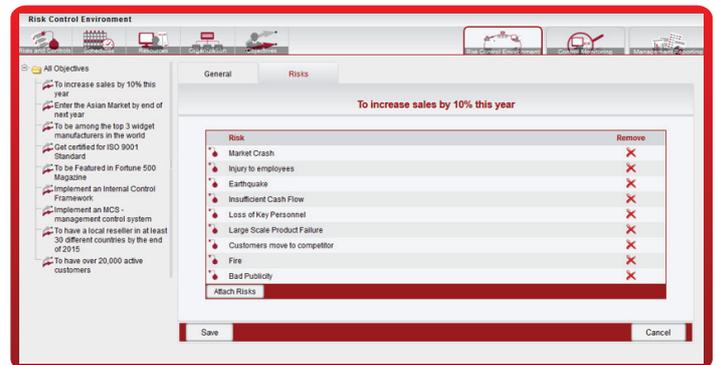
The COSO internal control framework 2013 has been an important influence in the development of Objective Controls. We had at one point considered making it a dedicated COSO implementation tool, but in the end we chose to pass on the made-to-measure approach and instead produce a less restrictive solution that

would help get people up and running fast with other risk and internal control management frameworks as well. Nevertheless, there's a lot of COSO-like thinking in our app and in this paper, I will present some of the essential aspects of Objective Controls through the context of COSO 2013.

I came to be a fan of the COSO Internal Control Framework the moment I laid eyes on it. One illustration of its conceptual simplicity that still grabs me is its definition of internal control, the purpose of which, it states, is to help management better control the organization. It adds that internal control is geared to the achievement of objectives and is a process of ongoing tasks and activities - a means to an end, not an end in itself. These concise but forceful words encompass what we strive for in Objective Controls too!

Objectives First

COSO squarely sets objectives in the upper facet of its 3-dimensional conception and goes about helping the organization achieve them using the method of internal control, a set of integrated rules and practices or components. Similarly, we put objectives at the top of the Objective Controls hierarchy as well and everything below them is part of a common goal to try and achieve them.



Entity Structure

Jumping to the other extreme of the COSO cube, we have a 4-level breakdown of an organization. In the COSO taxonomy, these levels are termed, entity, division, operational unit and function. When deciding how to dice up the organization in Objective Controls, we chose a more flexible multiple-level organizational tree structure in which each level is a generic organization unit and so it can be mapped to any organizational structure. COSO purists can map it exactly to COSO terminology while others can fit it to

their own organizational reality.

Despite their crucial importance in creating the status picture that will help people manage their organizations better, both objectives and entity structure have only a limited active role in the art of internal control and risk management. This is true both of the COSO Internal Control Framework and the Objective Controls software system.

Internal Control

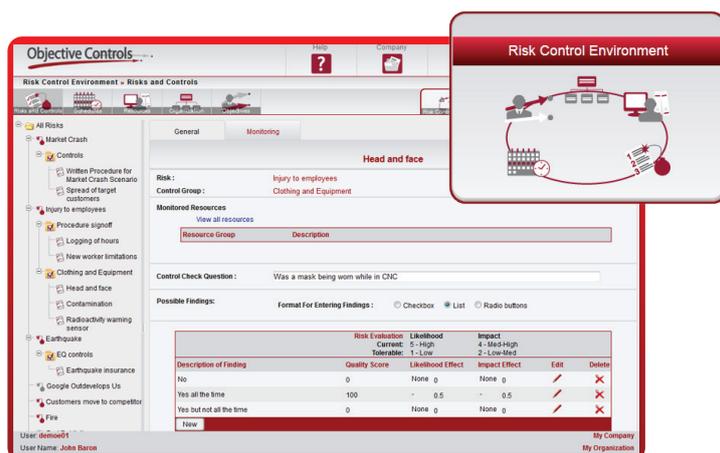
Now that we've looked at some similarities at the way the framework and the software relate to objectives and entity structure, we can focus our attention on the process of internal control, which is the center stage and main procedural part of the COSO Internal Control Framework on paper and of Objective Controls on a computing device.

COSO breaks the process of internal control down into 5 components: Control environment, risk assessment, control activities, information and communication and monitoring activities and this quintet is put into operation in an iterative and continuous way. The main girth of the COSO Internal Control Framework is taken up by its granular breakdown of these 5 components into 17 distinct 'principles'.

1 Control Environment

COSO has a control environment; Objective Controls has a 'risk control environment'. Both can be fairly described as a set of standards, processes and structures that provide the basis for carrying out internal control in the organization but due to the essential difference between a best practice framework and a software framework, each interprets control environment in a way that fits in best with its own fabric. COSO's control environment, as defined in the first 5 of its 17 principles, outlines management ideals, touching on commitment, ethics, behavior and accountability. Whilst these things are indeed essential ingredients of a healthy tone at the top and they fit in perfectly with a best practices approach, they have less value in a computerized framework like Objective Controls, which uses its risk control environment for definitions of the organizational components needed

to make the software processes work. These include risks, controls, schedules and assets that may later be observed in control monitoring activities.



2 Risk Assessment

The COSO internal Control Framework 2013 devotes principles 6 to 9 to the subject of risk assessment. This is the logical next step following the declaration of strategic objectives and COSO covers many angles of view in this part of its mission of identifying and understanding potential events that could adversely affect objectives. In their handling of risk assessment, Objective Controls and COSO 2013 share a number of common considerations, including the effect of risks on objectives, reviewing and reconsidering objectives, risk tolerance, risk response and others.

Both platforms leave the exact mechanisms for evaluating risks up to the organization itself due to the considerable variation of methods employed from one organization to another.

The differences between the nature of COSO as a best practice guide and that of Objective Controls as a software tool are seen here also; COSO discusses risk assessment from the angle of management issues such as fraud, leadership changes, mismanagement and attitudes, while Objective Controls is focused on documenting the assessment.

3 Control Activities

Objective Controls allows the organization to specify controls (or control activities) and tie them to the risks and objectives previously identified. COSO's principle 10 is exactly the background discussion that should feed the choice of controls defined in the software application.

Both COSO and Objective Controls drive the reader/user toward creating controls in order to steer the organization towards policies and procedures that will help achieve their objectives, giving controls the role of 'risk mitigators'. Principle 11 introduces technology as a means of control and even though the

focus is more on the impact of technology in the context of business processes than on computer systems to manage internal control, I think it's fair to suggest that risk and internal control management software can and should be included in this category too!

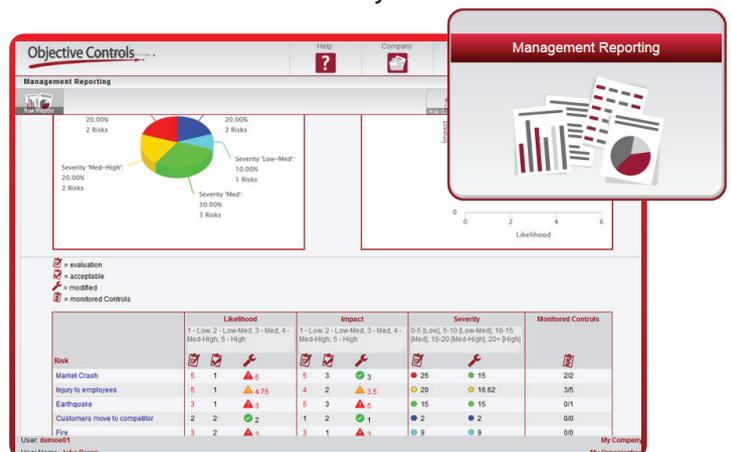
The framework brings its discussion on control activities to a close with mention of corrective action, timeliness, iteration and periodic reassessment and all of these are implemented in Objective Controls.

4 Information and Communication

In its introduction to the 4th its 5 components, COSO 2013 manages to put this all-encompassing ingredient of an organization's operation into perspective, both within and outside the context of internal control. It also describes an information system as a set of activities involving processes, people and data, which enables the organization to use transactions and information to measure progress towards the achievement of objectives. The same description can also be applied to the Objective Controls software application.

Principles 13 through 15 explore how information is used in the other 4 components of internal control and gives a variety of examples to illustrate the point. It touches on the people involved in the communication of information, quality of information and types of communication (dashboards, procedures, email and others). As with the other sections of COSO, some of the guidelines listed are high-level, leaning more to procedures and standards of behavior while others can be solidly implemented in a software application and

many of them are built into our computerized risk and internal control management solution. Specific examples of Objective Controls elements of information and communication include: Management dashboards, scheduling of control monitoring tasks, mapping of risks to objectives and vice versa, clearly specifying controls per risk and specifying the effects of different findings from control monitoring observations on risks and objectives.



5 Monitoring Activities

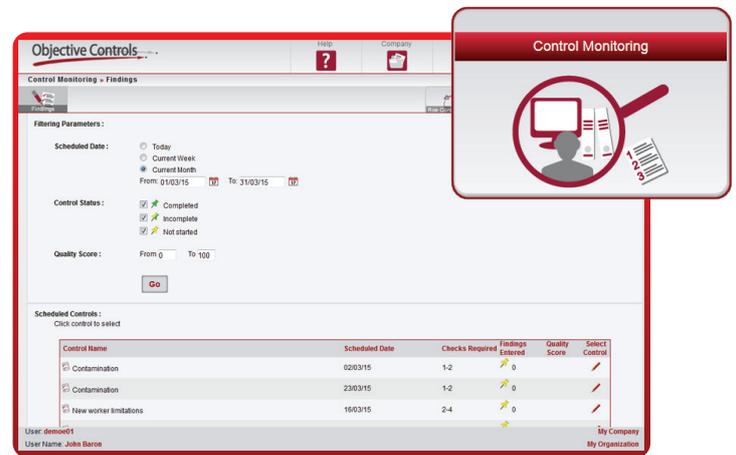
The fifth and final component of internal controls as defined in the COSO Internal Control Framework 2013 is perhaps the most essential process of the Objective Controls solution.

COSO makes the distinction between control activities and monitoring activities by referring to a control activity as a response to a specific risk whereas a monitoring activity is referred to as a way of checking whether internal control itself is operating as intended. The last two of COSO's seventeen principles deal with reviewing the internal control system as a whole.

In Objective Controls, control activities and monitoring activities are organized a little differently than in the COSO structure. We map these 2 activities to 3 distinct processes. The first is control definition where a user defines not just what the control is but also how it is to be monitored including the significance of possible findings that can be expected when the monitoring is done. The second process is the scheduling of the monitoring tasks for execution on explicit dates over the short or long term ahead; and the third is presenting the monitoring tasks to users who have

been given the monitoring role, along with an explanation of how they need to go about the task including the possible findings defined previously so they can select the one most appropriate. Finally, the chosen finding is recorded and saved.

If we are talking about monitoring or reviewing the entire internal control function, it is handled no differently than the activity of monitoring any other 'regular' control.



To summarize, Objective Controls is a computerized internal control system that has a lot of COSO-like thinking in it. For organizations interested in implementing COSO, it provides a practical way of automating some of the main processes of internal control according to COSO 2013 Internal Control Framework.

For more information about the COSO internal Control Framework 2013, visit <http://www.coso.org/ic.htm>

For more information about Objective Controls, visit www.objectivecontrols.com