

## COSO'S New Definition

There are eight components in COSO's new definition of the **Enterprise Risk Management** process. Five of them should be familiar to Internal Control practitioners.

|  |   |
|--|---|
| <b>Internal Environment</b>            | Reflects an entity's philosophy on risk management, considering performance and value ( <i>i.e.</i> , <i>cost of control vs. cost of risk</i> ) to arrive at an acceptable level of risk.   |
| <b>Objective Setting</b>               | Based on an entity's mission, management sets strategic objectives, which if achieved will create and preserve value for the organization.  |
| <b>Event Identification</b>            | Management identifies potential events affecting its ability to achieve objectives<br>Events with potentially <u>negative</u> consequences represent RISK.<br>Events with potentially <u>positive</u> consequences represent OPPORTUNITY.   |
| <b>Risk Assessment</b>                 | Management assesses likelihood and impact of negative events ( <i>qualitatively and quantitatively</i> ).   |
| <b>Risk Response</b>                   | Management identifies response options, taking into consideration cost versus benefit and acceptable level of risk. Responses may include avoidance, reduction, sharing of risk (e.g., pooling of risk or co-insurance), and acceptance of risk.<br><i>The chosen response(s) may have significant impact on the entity's business plan, services provided, product line or corporate policy.</i> |
| <b>Control Activities</b>              | Policies and procedures help ensure appropriate risk response, including activities such as approval, authorization, verification, reconciliation, review of operating performance, security of assets, and segregation of duties.  |
| <b>Information &amp; Communication</b> | Pertinent information from internal and external sources must be identified, captured and communicated in a timely and relevant fashion.<br><i>This includes exchange of relevant information among external parties, customers, vendors, regulators, stakeholders.</i>   |
| <b>Monitoring</b>                      | Monitoring assesses both the present and functioning of risk management components, as well as quality of performance over time.  |

COSO's draft ERM Framework will be available after July 15, 2003 at [www.coso.org](http://www.coso.org).

Document prepared by [www.lceman.com](http://www.lceman.com)