COSO Evolution

Internal control (Risk Management) is a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance (COSO ERM added strategic objectives).

IC 1992	ERM 2004	ICFR 2006	IC 2013
Objective Categories: E&E of Operations, Reliability of Financial Information, Compliance with Applicable Laws and Regulations	**Objective Categories:** Strategic, Operations, Reporting, Compliance	**Objective Categories:** Financial Reporting	**Objective Categories:** Operations, Reporting, Compliance
Control Environment	**Internal Environment**	**Control Environment**	**Control Environment**
• Integrity and Ethical Values • Board of Directors • Management’s Philosophy and Operating Style • Organization Structure • Commitment to Competence • Assignment of Authorities and Responsibilities • Human Resource Policies and Practices	• Integrity and Ethical Values • Board of Directors • Risk Management Philosophy • Organizational Structure • Commitment to Competence • Assignment of Authorities and Responsibilities • Human Resource Standards • Risk Appetite	• Integrity and Ethical Values • Board of Directors • Management’s Philosophy and Operating Style • Organizational Structure • Financial Reporting Competencies • Authorities and Responsibilities • Human Resources	• Integrity and Ethical Values • Board of Directors • Commitment to Competence • Structures, Reporting Lines, Roles and Responsibilities • Accountabilities for Internal Control Responsibilities
Risk Assessment	**Risk Assessment**	**Risk Assessment**	**Risk Assessment**
• Objectives • Risk Identification and Analysis • Managing Change	• Objective Setting • Event Identification • Risk Assessment • Risk Response	• Financial Reporting Objectives • Financial Reporting Risks’ • Fraud Risk	• Objective Setting • Risk Identification and Assessment • Fraud Risks • Impact of Changes
Control Activities	**Control Activities**	**Control Activities**	**Control Activities**
• Integrated with Risk Response • Top-Level Reviews • Direct Funcational or Activity Management • Information Processing • Physical Controls • Performance Indicators • Segregation of Duties • Policies and Procedures	• Integrated with Risk Response • Top-Level Reviews • Direct Funcational or Activity Management • Information Processing • Physical Controls • Performance Indicators • Segregation of Duties • Policies and Procedures	• Integration with Risk Assessment to Address Financial Reporting Risks • Preventive and Detective Controls and Segregation of Duties • Policies and Procedures • Information Technology	• Contribute to the Mitigation of Risks with Tranction Controls, Entity-Specific Controls, Segregation of Duties • IT Controls over Infrastructure, Access, Acquisition and Development • Policies and Procedures

Information and Communcation	Information and Communcation	Information and Communcation	Information and Communcation
• Pertinent information is identified, captured and communicated appropriate form and timeframe, both internally and externally • Systems produce reports that make it possible to run and control the business. • Effective communication also must occur in a broader sense, flowing down, across and up the organization.	• Information communicated in form and timeframe so people can carry out their jobs • Information is integrated with operations • Quality information is communicated internally and externally	• Financial information is used at all levels of the organization to support objectives • Inforamtion about internal control is distributed in appropriate form and timeframe • Quality of information is maintained	• Uses relevant and quality information regarding functioning of internal control • Communicates needed information internally • Communicates needed information externally
Monitoring	**Monitoring**	**Monitoring**	**Monitoring**
• Ongoing Monitoring by Management • Separate Evaluations • Reporting Deficiencies	• Ongoing Monitoring by Management • Separate Evaluations • Reporting Deficiencies	• Ongoing and Separate Evaluations • Reporting Deficiencies	• Ongoing and Separate Evaluations to Ascertain IC Components are Working • Evaluation and Communication of IC Deficiencies

The above was accumulated from *Internal Control - Integrated Framework* (IC 1992 and IC 2013)*, Enterprise Risk Management Integrated Framework* (ERM 2004), and *Internal Control over Financial Reporting* (ICFR 2006).

High-Level Changes (From Foreward of 2013 Executive Summary)

The experienced reader will find much that is familiar in the Framework, which builds on what has proven useful in the original version. It retains the core definition of internal control and the five components of internal control. The requirement to consider the five components to assess the effectiveness of a system of internal control remains unchanged fundamentally. Also, the Framework continues to emphasize the importance of management judgment in designing, implementing, and conducting internal control, and in assessing the effectiveness of a system of internal control.

At the same time, the Framework includes enhancements and clarifications that are intended to ease use and application. One of the more significant enhancements is the formalization of fundamental concepts that were introduced in the original framework. In the updated Framework, these concepts are now principles, which are associated with the five components, and which provide clarity for the user in designing and implementing systems of internal control and for understanding requirements for effective internal control.

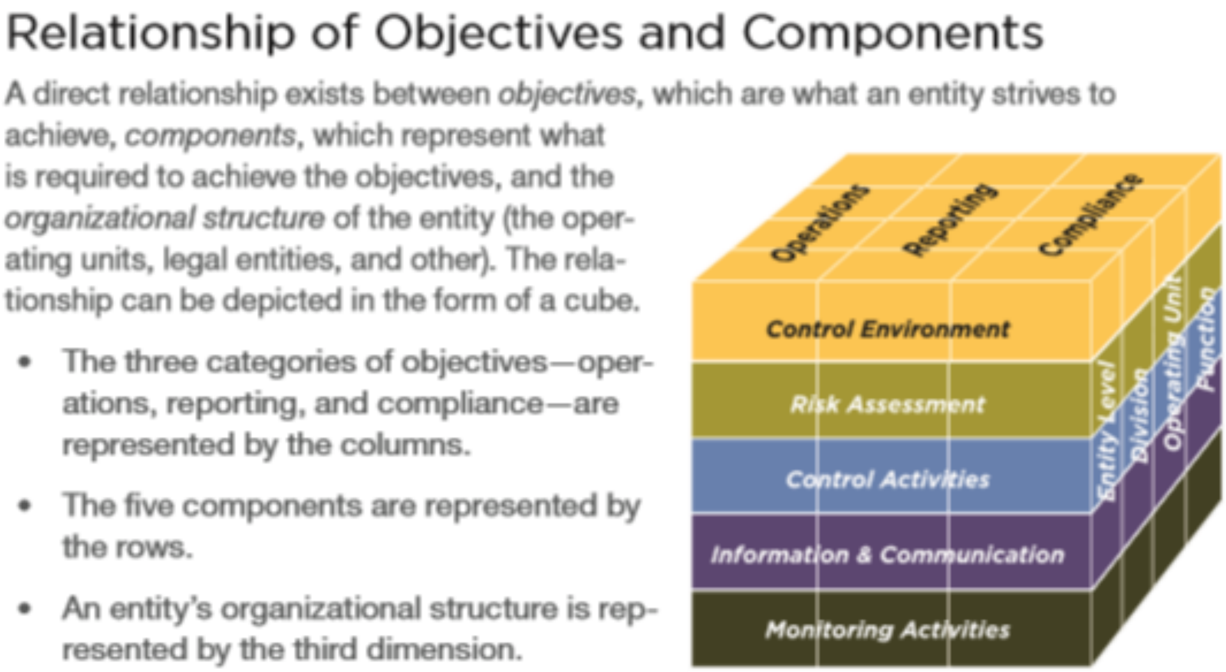
What's Available (From Foreward of Executive Summary)

This Executive Summary, provides a high-level overview intended for the board of directors, chief executive officer, and other senior management. The Framework and Appendices publication sets out the Framework, defining internal control, describing requirements for effective internal control including components and relevant principles, and providing direction for all levels of management to use in designing, implementing, and conducting internal control and in assessing its effectiveness. Appendices within the Framework and Appendices provide additional reference, but are not considered a part of the Framework. The Illustrative Tools for Assessing Effectiveness of a System of Internal Control, provides templates and scenarios that may be useful in applying the Framework.

In addition to the Framework, Internal Control over External Financial Reporting: A Compendium of Approaches and Examples has been published concurrently to provide practical approaches and examples that illustrate how the components and principles set forth in the Framework can be applied in preparing external financial statements.

COSO previously issued Guidance on Monitoring Internal Control Systems to help organizations understand and apply monitoring activities within a system of internal control. While this guidance was prepared to assist in applying the original framework, COSO believes this guidance has similar applicability to the updated Framework.

Among other publications published by COSO is the Enterprise Risk Management— Integrated Framework (ERM Framework). The ERM Framework and the Framework are intended to be complementary, and neither supersedes the other. Yet, while these frameworks are distinct and provide a different focus, they do overlap. The ERM Framework encompasses internal control, with several portions of the text of the original Internal Control–Integrated Framework reproduced. Consequently, the ERM Framework remains viable and suitable for designing, implementing, conducting, and assessing enterprise risk management.



Relationship of Objectives and Components

A direct relationship exists between *objectives*, which are what an entity strives to achieve, *components*, which represent what is required to achieve the objectives, and the *organizational structure* of the entity (the operating units, legal entities, and other). The relationship can be depicted in the form of a cube.

- The three categories of objectives—operations, reporting, and compliance—are represented by the columns.
- The five components are represented by the rows.
- An entity's organizational structure is represented by the third dimension.

Effective Internal Control (Pg 8 of Executive Sumary)

The Framework sets forth the requirements for an effective system of internal control. An effective system provides reasonable assurance regarding achievement of an entity's objectives. An effective system of internal control reduces, to an acceptable level, the risk of not achieving an entity objective and may relate to one, two, or all three categories of objectives. It requires that:

- Each of the five components and relevant principles is present and functioning. "Present" refers to the determination that the components and relevant principles exist in the design and implementation of the system of internal control to achieve specified objectives. "Functioning" refers to the determi- nation that the components and relevant principles continue to exist in the operations and conduct of the system of internal control to achieve specified objectives.
- The five components operate together in an integrated manner. "Operating together" refers to the determination that all five components collectively reduce, to an acceptable level, the risk of not achieving an objective. Components should not be considered discretely; instead, they operate together as an integrated system. Components are interdependent with a multitude of interrelationships and linkages among them, particularly the manner in which principles interact within and across components.

When a major deficiency exists with respect to the presence and functioning of a component or relevant principle, or with respect to the components operating together in an integrated manner, the organization cannot conclude that it has met the requirements for an effective system of internal control.

More on Requirements for Effecive Internal Control (From Pg 173 of the Framework)

The Framework requires that each of the components and relevant principles be present and functioning and the five compoents be operating together.

Sarbanes-Oxley Transition (See http://www.coso.org/newsroom.htm)

Article Discusses Transition to 2013 Internal Control — Integrated Framework for Sarbanes-Oxley Section 404 Compliance

COSO has issued an article aimed at assisting public companies comply with Section 404 of the U.S. Sarbanes-Oxley Act of 2002. The article outlines an example of one approach to transitioning to COSO's 2013 Internal Control–Integrated Framework (Framework) from the original framework published in 1992.

Read Press Release
Read Article

COSO believes that users should transition their applications and related documentation to the updated Frameworkas soon as is feasible under their particular circumstances. As previously announced, COSO will continue to make available its original Framework during the transition period extending to December 15, 2014, after which time COSO will consider it as superseded by the 2013 edition. During the transition period (May 14, 2013 to December 15, 2014) the COSO Board believes that organizations reporting externally should clearly disclose whether the original Framework or the updated Framework was utilized.

The 2013 COSO Framework & SOX Compliance

ONE APPROACH TO AN EFFECTIVE TRANSITION

By J. Stephen McNally, CPA

Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance (COSO ERM added strategic objectives).

The COSO Framework sets out five components of internal control and seventeen principles representing the fundamental concepts associated with components. These components and principles of internal control are suitable for all entities. All seventeen principles apply to each category of objective, as well as to objectives and sub-objectives within a category.

Internal or Control Environment (5 principles) - the CE is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The board of directors and senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct.

1.1 Integrity and Ethical Values. The organization demonstrates a commitment to integrity and ethical values (Codes of conduct, values statements, principles, ethics in dealing with others, procedures to determine ethical compliance)	
1.2 Independent BOD. The board demonstrates independence from management and exercises oversight of the development and performance of internal control. (Frequency of challenges to management, interactions with auditors and with management, direction given to external auditors, level of independence, clarity of charters, Board evaluation of Audit Committee, role in whistle- blowing procedures, reviews of financial information, clarity of governance processes)	
1.3 Roles and Responsibilities. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. (Organization charts, self-directed work teams, project teams, quality circles, focus groups, committee structures, organizational design functions, limits of authority, approval processes, controls over management overrides, delegations of authority, accountability mechanisms, responsibility matrices)	
1.4 Commitment to Competence. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. (Analysis of skills required, job descriptions, training and development efforts, professional development programs, mentoring and coaching programs, succession planning, employment contracts, career planning efforts)	
1.5 Accountabilities. The organizations holds individuals accountable for their internal control responsibilities in the pursuit of objectives. (Organization-wide human resource policies and standards, hiring and selection procedures, employee termination procedures, salary and bonus systems, background checks, personnel evaluation systems, upward and 360 feedback processes, employee self- assessment processes, remedial actions toward policy violations)	
ERM 1.6 COSO ERM Added: Risk management philosophy, appetite, culture and tolerance	

Risk Assessment - Objectives, Risks, and Responses (4 principles) – Risk assessment involves a dynamic and iterative process for identifying and analyzing risks to achieving the entity’s objectives, forming a basis for determining how risks should be managed. Management considers possible changes in the external environment and within its own business model that may impede its ability to achieve its objectives.

2.1 Objective Setting. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. (Mission statements, vision statements, strategic and directional objectives, business plans, departmental plans, tactical planning, SMART objectives, prioritization of objectives)	
2.2 Risk Identification and Assessment. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. (Mechanisms, discussions and meetings to identify internal and external risk events; estimating likelihood and impact of potential risks; procedures to consider what could go wrong at entity- and activity- and process-levels; management making decisions to accept, avoid, reduce or share risks based on cost, benefit, impact and likelihood)	
2.3 Fraud Risks. The organization considers the potential for fraud in assessing risks to the achievement of objectives. (Fraud committee activities, identification of risks due: asset misappropriations, corruption, fraudulent statements; fraud workshops; fraud prevention programs)	
2.4 Impact of Changes. The organization identifies and assesses changes that could significantly impact the system of internal control. (Mechanisms, discussions and meetings to identify risks due to changing conditions)	
2.5 COSO ERM Added: Distinguishing risks and opportunities and a portfolio view of risks.	
Note: Management making decisions to accept, avoid, reduce or share risks based on cost, benefit, impact and likelihood is part of internal control, but the actions undertaken to share or reduce the significance or likelihood of a risk (that is, risk responses) are part of the management process, not an element of internal control. But, for clarity, examples of these actions are shown below as Control Activities, and can be directly associated with risks identified in the Risk Assessment component.	

<u>Control Activities (3 principles)</u> – CA’s are the actions established by policies and procedures to help ensure that management directives to mitigate risks to the achievement of objectives are carried out. CA’s are performed at all levels of the entity and at various stages within business processes, and over the technology environment.

3.1 Activities that Mitigate Risks. The organization selects and develops CA’s that contribute to the mitigation of risks to the achievement of objectives to acceptable levels (Reconciliations, physical safeguarding and access controls, comparisons, validity tests, proper forms design, insuring against losses, bonding of personnel, transaction and credit limits, segregation of incompatible duties, secondary reviews)	
3.2 IT infrastructure controls. The organization selects and develops general controls activities over technology to support the achievement of objectives. (General and application controls; program development and change controls, access controls to programs and data, computer operations controls, tests of IT contingency plans; passwords and user identifiers and privileges; areas defined in COBIT and Global Technology Audit Guide (GTAG) control models process flow controls; manual and automated controls over how transactions are initiated, authorized, recorded, processed and reported; matching of documents; controls to ensure complete, accurate, authorized, timely and safeguarded transactions)	
3.3 Deployment through Policies and Procedures. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action. (Procedure manuals, desk manuals, instruction books; help screens; annual and long-term budgeting procedures; standardized contracts; disaster recovery plans; approvals, authorizations, verifications defined in policies and procedures; analytical analyses, relating operating and financial data; investigating results; comparing different data sources; financial and competitor trend analysis, organization-wide reviews and monitoring of budgets, earnings meetings, reviews of operating results, disclosure committee activities, reviews of public reports by management, other reviews of organization functions, operations, or procedures; controls over period-end financial reporting, tests of company- wide disaster recovery plans, formal document retention schedules, Federal Acquisition Regulations, Joint Commission on Accreditation of Healthcare Organizations (JCAHO) standards; national and regional accreditation for universities; controls specific to certain industries, chart of accounts structures)	
Note: some management initiatives are full-scale methodologies designed to achieve business objectives. Examples of these initiatives are shown below as control activities, but in practice they supply controls to all the COSO components. If present in an organizational unit, their activities and controls can be mapped to the relevant COSO components to provide a consistent framework for an evaluation of control across the whole organization.	
Other 3.4 Management and quality initiatives designed to help achieve business objectives. For instance ISO 9000, 10000, 14000, 31000 certifications; Malcolm Baldrige quality programs; Total Quality Management efforts; Balanced Scorecard systems, Enterprise Risk Management; compliance with Sarbanes-Oxley and Basel Accords; Management by Objectives; Six Sigma programs; Occupational Health, Safety and Environment programs; Learning Organizations; Key Performance Indicators (KPI) and Key Success Factor (KSF) programs; security, legal and regulatory compliance functions.	

<u>Information and Communication (3 principles)</u> – Information is necessary for the entity to carry out internal control responsibilities in support of achievement of its objectives. Communication occurs both internally and externally and provides the organization with the information needed to carry out day-to-day controls. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of objectives.

4.1 Indicators and Measurements. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control. (Metrics, key performance indicators, measures and scorecards of performance, dashboards, benchmarking studies, heat maps, market share reports, competitor analysis)	
4.2 Internal Communications. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. (Suggestion boxes, personnel announcements, internal newsletters, discussion boards and bulletin boards of company events, intranet websites and portals; formal policy and procedure systems; management guides; internal survey processes; scheduled management presentations; open forum meetings, all hands and departmental meetings; video and telephone message broadcasts; executive lunches with employees, internal whistle-blowing mechanisms; separate lines of communication; management messages about security, ethics, citizenship, policies, risks, controls, policies, objectives, strategies, values)	
4.3 External Communications. The organization communicates with external parties regarding matters affecting the function of internal control. (Customer forums, external surveys, analyst meetings, external websites, publications and newsletters, hotlines)	
App 4.4 Most business areas depend on an underlying IT application. Such applications are also internal controls.	

<u>Monitoring (2 principles)</u> – Ongoing evaluations, separate evaluations or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to effect the principles within each component, is present and functioning. Findings are evaluated and deficiencies are communicated in a timely manner, with serious matters reported to senior management and to the board.

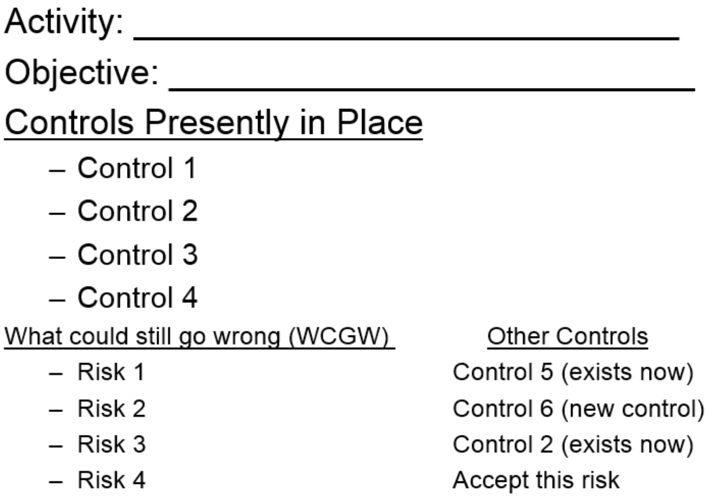
Note: Monitoring in COSO relates to assessing the operation of internal control and risk management processes, as opposed to Control Activities such as top-level reviews, forecasts and budgets which are entity-wide control activities.

5.1 Ongoing and Separate Evaluations of Components. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. (asking questions while walking around, discussing controls with employees, talking with customers about employee conduct, supervisor observations, periodic reviews by internal auditors, external auditors, regulators, ISO auditors, specialists; accreditation reviews; OSHA reviews; examiners; security reviews)	
5.2 Reporting of Deficiencies in Control. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. (Follow-up on control gaps and problems that occur; open issues lists; status reporting on audit and other reviews and studies; fraud reporting and investigation mechanisms; reviews of policies and procedures for continued relevance)	

The above was accumulated from *Internal Control - Integrated Framework (2013)* and *Enterprise Risk Management (ERM) Integrated Framework* (2004).

<u>Application of COSO Template</u>

- Step 1. Entity-Level Controls. Use the COSO Template to identify the specific controls in place for each entity (group of people). Each entity should have all the applicable 5 Components and 17 Principles present.
- Step 2. Activity-Level Controls. For each major activity an entity performs, use a Residual Risk Matrix (format below) to determine if all risks have been adequately mitigated, considering the Entity-Level and Activity-Level Controls in place.



Activity: ______________________________

Objective: _____________________________

<u>Controls Presently in Place</u>

– Control 1

– Control 2

– Control 3

– Control 4

<u>What could still go wrong (WCGW)</u>	<u>Other Controls</u>
– Risk 1	Control 5 (exists now)
– Risk 2	Control 6 (new control)
– Risk 3	Control 2 (exists now)
– Risk 4	Accept this risk