Larry's Cheat Sheet – COSO 5 Components and 17 Principles

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.

Control Activities (3 principles) – 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)

Larry@LHubbard.com
+1(301) 529-8118
Larry Hubbard & Associates

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.

Information and Communication (3 principles) – 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.

Monitoring (2 principles) – 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).

Larry@LHubbard.com
+1(301) 529-8118
Larry Hubbard & Associates