

Larry's Cheat Sheet – COSO

References and Guidance
<p>Standards: Committee of Sponsoring Organization's (COSO) <u>Internal Control – Integrated Framework</u> (1992), <u>ERM – Integrated Framework</u> (2004), <u>Guide for Smaller Companies</u> (2006)</p>
<p>Definition: 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 in the following categories:</p> <ul style="list-style-type: none"> Effectiveness and efficiency of operations Reliability of financial reporting Compliance with applicable laws and regulations <p>From Internal Control – Integrated Framework (COSO I/C).</p>
<p>COSO ERM Cube and COSO IC Pyramid</p>

- ERM and IC both mean management has a “flow of reliable information” about each component of control for all the objectives, from all areas of the organization. It does not matter who provides the information as long as it is accurate and acted on.
- A basic risk framework: Internal risks, External risks, Risks due to changes works just fine to discuss risks – the discussion IS the control.

Predicting Success - Organizational Readiness **

Question	Score (0 to 5)
1. To what extent are department managers ready to involve employees in the ongoing identification of objectives, risks and controls for their activities?	
2. To what extent are department managers ready to receive and act on soft control information from their employees?	
3. To what extent is IA ready to gather and provide information about soft controls?	
4. To what extent is executive management ready for IA to help managers with internal control rather than play a police role?	
5. To what extent are audit managers ready to change to a single, new definition of internal controls and risks and new way of evaluating controls?	
6. To what extent are IA's ready to work with employees in the development of objectives, risks and controls?	
Total	

Range Chance of Success

0 to 10	20%
10 to 20	40%
20 to 30	80%

Tips about Controls and Risks:

- Some controls impact people's attitudes (entity); other controls are related to things people do (activities).
- Entities do activities with tools – all can be audited, but “people” are where the problems are.
- IC and ERM are a “company-thing” not an “audit-thing”.
- Internal Control and ERM are like two sides of coin.
- If other groups have internal, self-assessment processes, give them room to work. Audit somewhere else.
- ERM is a management task; RA is a component of both COSO's IC and ERM frameworks and RA is also how IA selects audits to perform (confusing!)
- It doesn't matter how much the IA's know about risks – only what workers know and care about matters.
- In doing risk assessment:
 - Don't confuse risk causes with risk impacts.
 - A risk is different than an objective containing a “not”
 - Controls that don't work are not “risks” – they are ineffective controls.
- Risk assessment starts with clarity of the objective.
- ERM and IC are all about achieving business objectives

**To successfully implement COSO IC or ERM framework

Successful Implementation Means

- Workers in all parts of the business voluntarily and regularly participate in the evaluation of their own internal controls, all the components.
- Information, even bad news, about internal controls is easily and truthfully gathered and shared upwards and across the organization, and corrected.
- Managers and workers identify and assess new risks, on an ongoing basis, and address them.
- All the above is happens without internal audit intervention. Auditors monitor the process and determine if the flow of control information is working as intended.

Copyright © 2007 Larry Hubbard

Larry's Cheat Sheet – COSO

- COSO Internal Environment (AKA Control Environment) – How likely are people to perform internal control responsibilities?
 - Management philosophy (statements of tone at the top; messages about importance of people, implied or actual pressure to achieve results; endorsed management principles, attitude toward: controls, financial reporting and auditing, responses toward policy violations)
 - Ethics and values (codes of conduct, values statements, ethics in dealing with others)
 - Company structure and assignment of authority (limits of authority, centralized vs. shared processes, approval processes)
 - Commitment to competence (job analysis, job descriptions, training and development efforts, professional development programs, feedback programs on values and ethics and conduct, personnel evaluation system, upward and 360 feedback processes)
 - Company-wide policies (HR standards, bonus systems, fraud prevention programs, background checks, ERM programs)
- BOD and Audit Committee activities (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, whistle-blowing procedures, reviews of financial information, clarity of governance role)
- Accounting Policies and Procedures (accounting policy and procedure manuals, disclosure committee activities, reviews of public reports by management)
- Company-wide monitoring (budgeting, monitoring of results, earnings meetings, IT policies)
- IT application controls (procedures to prevent and detect unauthorized transactions; controls to ensure complete, accurate, authorized, timely and safeguarded (CAATS) transactions; security systems to implement segregation of duties and protect data)
- Process flow controls - how transactions are initiated, authorized, recorded, processed and reported
- Business contingency planning and recovery procedures

Control Activities – Policies and Procedures – How does management know if risk responses are working?

- Segregation of incompatible duties; physical counts
- Policies, procedures, desk manuals
- Reconciliations, approvals, authorizations, verifications
- IT general controls (Program development and change controls, access controls to programs and data, computer operations controls, COBIT control model)
- Tests of contingency plans
- Other frameworks: ISO 9003, Malcolm Baldrige, TQM, Six Sigma

Information and Communications – Do people get the information they need to know about achieving objectives.

- Metrics, key performance indicators, measures and scorecards of performance
- Management presentations, open forums, all hands meetings, newsletters, intranet websites
- Messages about security, ethics, citizenship, policies
- Newsletters, discussion boards of company events, suggestion boxes

Monitoring and Oversight – What procedures help determine if the other control components are working?

- On-going supervisor activities to see if things worked right
- Periodic reviews by auditors, examiners, etc.
- Reporting and correction of known problems

Derived from COSO's Internal Control and, Enterprise Risk Management Frameworks and Smaller Company Audit Guide.

Copyright © 2007 Larry Hubbard
Larry@LHubbard.com
(301) 529-8118

Risk Assessment - Objectives, Risks, and Responses – What Could Go Wrong (WCGW) – How much do people know about entity (people-related) and activity (process-related) objectives, risks and responses?

- Clarity of objectives (mission statements, high-level objective statements, published strategic objectives, meetings about objectives)
- Identification of internal and external risk events (discussions of what could go wrong, fraud risks)
- Prevent and detect responses to identified risks