

Using the COSO Map

Unpublished Article
By Larry Hubbard

Internal Control – Integrated Framework published by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission – How many times have we read articles containing that phrase? And how many times have we all seen the COSO pyramid and the COSO cube? Many times for all of us. Well, this is NOT just another COSO article.

I have talked with hundreds of internal auditors, attended and taught countless conferences and seminars, reviewed many Sarbanes-Oxley Section 404 approaches, and even helped companies implement Enterprise Risk Management. In doing these things, it is clear that many people are still looking for a practical way to use the COSO framework. Having also spent considerable time with the major COSO documents (IC, ERM, Small Company, and now Monitoring), I know it is possible to piece together management controls, internal controls, control design adequacy, and control effectiveness, into a practical approach to identifying controls that is consistent with COSO. This article describes how those concepts fit together.

Start with Management Controls

All managers do things to help be sure jobs, or activities, are done the right way. For instance, they hire the right workers; provide workers with training; evaluate performance; insert approvals and reviews in the activity; establish performance metrics; communicate objectives and other job expectations; and monitor the work done. These “things” or “management controls” are not the actual steps of doing a job or activity – these management controls come before, or during, or after the actual steps of a job. That is, workers do the actual job steps, or tasks or activities, and controls are things before, during or after an activity that help the activity go right.

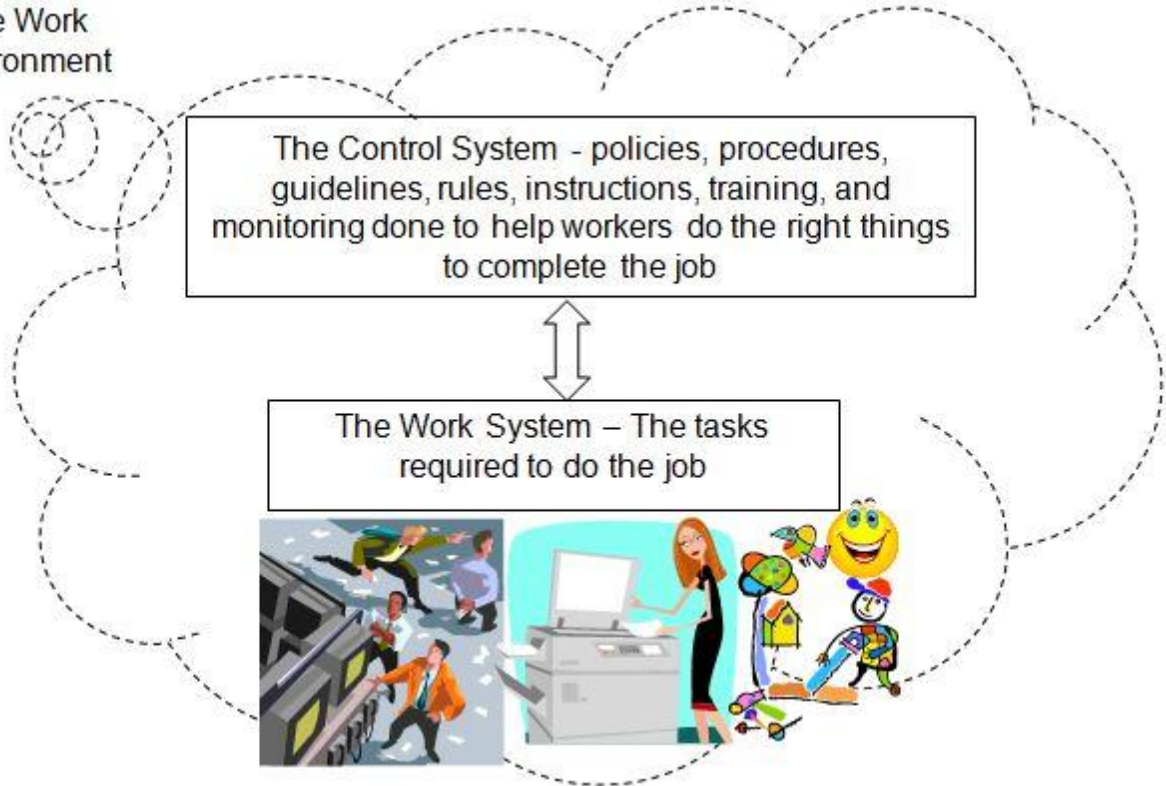
Any activity has both “actual job steps” and things that management installs to help be sure the activity goes right. My term for these “things” is management controls – although managers usually don’t call them controls at all. Based on their own backgrounds, the skills of their workers, existing procedures, and other factors, managers identify and implement these management controls to be sure activities go right.

In pictures, we can think of it this way. Every activity has three levels:

- the work system, which are the tasks required to do a job
- the management control system, which overlays the work and are the policies, procedures, guidelines, rules, instructions, training and monitoring that management establishes to help be sure the job is done correctly.
- the “work environment” that impacts the way people do their jobs. Managements’ attitude, philosophy, and commitment to competence; the organizational structure; the clarity of roles and responsibilities; the human resource system; the risk appetite and other broad-based attributes impact the way employees interpret both their job duties and importance of the control system.

Using the COSO Map

The Work Environment



Sometimes, controls are looked at as "part of a process" because of the way the business process has been designed. For instance, in a shipping activity, requiring that new customer orders receive credit approval prior to shipment is "part of the process" in some organizations. The reason it is called a "control" is that credit checking is not part of the actual shipping of the product - it is embedded in the shipping process, but it was put there by management to ensure the process works right. That is, we could sell to anybody and just hope we get paid, but instead we do credit checks to enhance the probability that we will get paid. Many steps, such as reconciliations and approvals and balancing, are embedded in business processes or activities - but they are put there by management to help "control" the process and be sure it works as planned. It really does not matter if we call those Management Controls or Internal Controls, or just "controls," but it is important to understand the function of controls is to help the actual job steps work correctly.

Identifying Management Controls

Identifying management controls is a four-step process:

1. Identify the major steps of the activity – three or four steps at most.
2. Identify the process flow controls – that is the things inserted into the activity to be sure those steps are done correctly.
3. Identify the non-process flow controls – training, hiring practices, guidelines, instructions that are before or outside of the actual flow of the activity, but are essential to being sure the activity is done right.
4. Ask what else could go wrong, despite the controls identified above – these can be called risk assessment controls.

Using the COSO Map

The order of the steps in this process for identifying management controls is important, and each step builds on the previous step. It is especially critical that the fourth step, asking about what else could go wrong, is done at the end of the process not at the start. If “what could go wrong” is asked before identifying the other controls it will take much longer, be a very negative process (looking for only bad things) and not give credit to management for the controls they already have in place.

The key to good internal auditing is to involve workers and managers in these four steps in a positive, interactive way. Step 2, identifying process flow controls, requires an especially high level of knowledge in the actual process steps. Auditors cannot be experts in every important activity of the organization, so worker and manager participation is essential. To get participation from audit “clients”, the control identification process must be efficient, logical, and positive (that is, not a negative exercise). These four steps, in the order provided, can provide that opportunity. Auditors that begin control identification by first asking risk assessment or “what could go wrong” questions never get the same level of participation from clients as those who approach control identification from a positive angle. It somewhat technical terminology, this is an inherent risk approach (first asking what could go wrong) vs a residual risk approach (first identifying controls in place, then asking what else could go wrong).

Another key is to be sure managers and workers know we auditors are not there to critique or criticise how people do their jobs. Auditors that have a high level of experience in a particular activity may be seen as “experts” in the actual job steps, and the workers may feel threatened or reluctant to share the controls they have in place. Although some audit departments do have a high level of expertise in selected critical activities of the organization, audit shops don’t have sufficient expertise, or staffing, to carry that “expert” designation in every important activity. Thus, we need a “process” to employ in identification of management controls. These four steps provide that process.

Turning Management Controls into Internal Controls

If the experts in organizational activities are in the business areas, not in the audit department, then how can auditors determine if the design of controls in an activity is adequate? That is, how can an auditor, who may know very little about an operational area, complex accounting function, or scientific area possibly say management has put the correct controls in place? Once all the process flow, non-process flow and risk assessment controls have been identified, how does the auditor evaluate the adequacy of the control design? The answer lies in something called a framework.

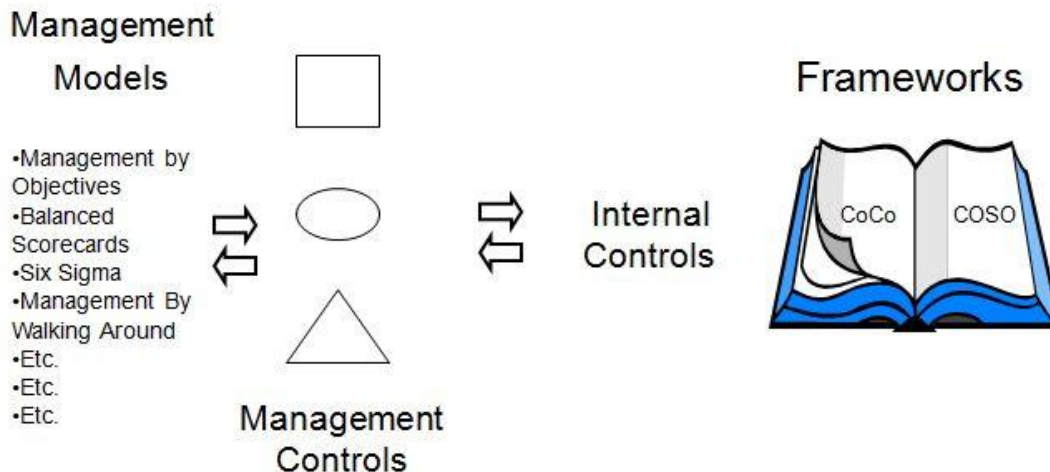
An internal control framework is a tool developed to help evaluators of control, like auditors, determine if there are enough, and the right kind of, management controls. It is simply an accepted set of guiding principles, or components that form a template against which to evaluate the many methods managers use to be sure activities go right. A framework is composed of various concepts, values, factors, and practices intended to assess or evaluate management controls.

Evaluators use various specific frameworks to assess the design adequacy of management controls. They form an alphabet-soup of C's: COSO, CoCo, Cadbury, COBIT, and others. We focus in this article on the COSO framework from the US, but any Internal Control framework has the same purpose. The other frameworks above are from Canada (CoCo), the UK (Cadbury), the IT Governance Institute (COBIT), and South Africa (King). And, while auditors

Using the COSO Map

sometimes say we are using these frameworks to evaluate internal controls, the frameworks were developed to compare or map existing management controls to the internal control framework so that auditors can evaluate the design of management controls against a consistent template across an organization. The fact that a framework is a comparison tool, not a management tool, is a critical concept.

Of course, managers need to understand the "framework" evaluators such as auditors will use to evaluate the design of controls, because managers must address any control design deficiencies when comparisons are made to that framework. However, managers don't use or adopt a control framework to manage their functions, even one as popular as COSO. That's not the purpose of a framework. Managers will continue to manage the ways that work best for them, or use the management models, such as Six Sigma or TQM, chosen by the organization. COSO is for auditors, evaluators, senior managers, and board, so they can produce consistent reports on controls, not for managers to use in managing their activities. Sure, auditors can teach COSO to workers and managers so the control evaluation process can go more smoothly, and maybe that discussion will yield additional, value-added, management controls. However, managers do not control business activities, or achieve business objectives, using COSO! In pictures, it looks like the following.



Another key concept is that auditors use internal control frameworks to evaluate management controls, not to evaluate the actual flow or steps of an activity. Evaluating the actual steps of an activity is far beyond the capability of any control framework.

Using the COSO Map

The process of comparing management controls to a framework is a mapping process. We are "mapping" what management does to be sure the right things happen in an activity to the components, or parts, of the framework. After mapping the management controls, if all the parts of the framework have specific controls identified, then we can say management controls are adequately designed when compared to the chosen internal control framework. So, the mapping process needs to be quite rigid in that a management control should map to one type of control

Using the COSO Map

in the framework. This is more difficult than it sounds, and something that most auditors don't do well, or have never really done.

I started this article by mentioning Internal Control – Integrated Framework, or the COSO IC framework. The Committee of Sponsoring Organizations (COSO) also developed another framework for Enterprise Risk Management, or the COSO ERM framework, and another to help in Sarbanes-Oxley Section 404, the COSO Small Company guide. Of course there are slight differences in all these documents, but the concepts of them all are the same. In fact, COSO Small Company is a simple regrouping of the COSO Internal Control components and factors into twenty principles related to internal controls over financial reporting (ICFR) along with examples related to smaller companies financial reporting. COSO ERM is a bit broader than COSO IC, by including additional objective categories, and offers more specifics about one component of internal control, the Risk Assessment component. But, COSO IC is fully incorporated into the COSO ERM framework. COSO has also issued a guide related to the Monitoring component of internal control. All this guidance is about five parts, of components, of internal control, and if someone understands how to apply the COSO IC framework they also understand the other documents. Also, COSO is applied to both entities (or groups of people) and activities (the things or activities people do). This understanding is essential to using COSO to evaluate the design of management controls.

To efficiently evaluate management controls using the COSO framework requires two tools: 1. The COSO Map for entity-wide, or entity-level, controls; and 2. A risk/control matrix for activity level controls.

Example of COSO Mapping

The COSO Map is simply the five components of COSO, plus examples of the controls within each component. It provides a detail list of factors that auditors can use to match management controls to, so they can be sure all components of internal control are covered. In the example below, a list of controls is provided. In an audit, the auditors would identify these controls through discussions with management and workers

Control	COSO Component Number	Entity-wide or Activity-level	Reasoning
a. Monthly publication of organizational changes	1.5 Organizational Structure 4.1 Newsletter	Entity-wide	1.5 – indicates there is an established organization chart 4.1 – indicates an ongoing method of communicating within the organization
b. Reconciliation of bank account to company's books	3.1 Response - Reconciliation	Activity-level	Reconciliation responds to the risk "items going through the bank, but not through the books" to achieve the objective

Using the COSO Map

			“ensure all transactions are recorded.”
c. Team meeting to discuss their objectives	4.1 Team Meeting 2.2 Objectives	Activity-level	2.2 – Indicates team, or activity-level, objectives are in place 4.1 - Indicates an ongoing communication process
d. External audit of the financial statements	5.2 External audit	Entity-wide	Indicates a separate periodic review by external auditors
e. Notification to vendors of company's policy that employees cannot accept gifts	1.1 Policy to not accept gifts 4.2 Notification to vendors	Entity-wide	1.1 – demonstrates ethics in dealing with others. 4.2 – indicates a process to contact and communicate with vendors.
f. Card access system to restrict access to office space	3.1 Card access system	Activity-level	Responds to risk “unauthorized access” to achieve activity-level objective “safeguard assets”.
g. Credit check before selling goods on credit	3.1 Credit check	Activity-level	Responds to risk “customers may default on sales invoices” to achieve objective “collect money for all sales.”
h. Batch balancing of input documents at data entry time	3.2 Batch balancing	Activity-level	Responds to risk “documents may be lost” to achieve objective “record all transactions.”
i. Feasibility study before developing a new product	1.8 Use of feasibility studies or 3.1 Feasibility study	Entity-wide Activity-level	1.8 – If used for all major new products indicates management’s low appetite for taking risks – they do not just “jump in”. 3.1 – If used on a single project,

Using the COSO Map

			responds to risk “product may not be accepted by market” to achieve objective “maximize revenue.”
j. Separating purchasing from receipt of goods	3.2 Segregation of duties	Activity-level	Responds to risk “fraudulent purchasing” to achieve objective “safeguard assets” or “Ensure goods purchased are for company usage.”
k. Orientation program for new employees	1.2 Orientation program	Entity-wide	Indicates commitment to developing people through training
l. Formal job descriptions for company positions	1.2 Job descriptions	Entity-wide	Indicates commitment to having competent people in right jobs
m. Awards for good performance	1.7 Awards	Entity-wide	Indicates a salary and bonus system to reward good performers
n. Discussions with employees of their career development plans and potential	1.2 Career development plans 4.2 Discussions	Entity-wide	1.2 – Indicates commitment to having competent people in right jobs 4.1 – Indicates a formal communication process with employees about their future
o. Decision by management to enter a new market, even though competitors have decided not to enter that market	2.1 Objective setting	Entity-wide	Indicates management setting objectives they feel are right for the organization.

Using the COSO Map

p. Comparing budget to actual expenses each month	3.1 Budget to actual comparison or 3.6 Company-wide budget comparisons	Activity-level Entity-wide	3.1 – For an individual department, responds to risk “unauthorized expenditures” to achieve objective “stay within budget” 3.6 – For an organization-wide effort, indicates a top-level review of budgets to actual.
q. Establishing and monitoring an annual Capital Expenditures Budget for the organization	3.6 Capital expenditures budget for organization	Entity-wide	Indicates to top-level, entity-wide review
r. A manager asking employees to save money by flying economy class, and then flying business class on their own trips.	4.4 Saying one thing, and doing another	Activity-level	Indicates a style of communication that might undermine the intended message.

The next step in the COSO Map would be to identify if any major components of the COSO Map do not have controls identified for them. If some important areas of the COSO Map don't have controls, the auditors would conduct more interviews or ask specific questions to determine if controls were present. In the above example, some activity-level controls are identified. Typically, a risk and controls matrix, not the COSO Map, is the best tool to document and identify activity-level controls.

Of course, determining whether or not there are sufficient Management Controls designed to support the factors in each component of the Internal Control framework, and the framework as a whole, is a decision based on experience and judgment, and one that evaluators must be prepared to explain to managers of the activity. Because, if management controls come up short when compared to the framework, the evaluators are going to report to senior managers and the board that additional controls must be implemented. When evaluators tell the board that managers, who are responsible for the activities' and the organization's success, have not designed enough controls into their activities, it is a serious charge. Such a statement must be objective, and must be supported by more than simply the evaluator's judgment or feeling that more controls are needed. As smart as we auditors are, managers and their workers will always know more about their business activities, and what makes them run right, than we do. An IC framework is the common denominator, or common definition, designed to provide an objective measuring stick across all the activities of an organization and the many different management models, to provide a consistent, unbiased basis for reporting to senior managers and the board on management controls.

Using the COSO Map

The COSO Map is best used to identify entity-wide, or entity-level, controls that relate to or impact to people (or “entities”). Another tool, a risk and control matrix, can then be used to identify specific risks and controls for an activity. Identifying entity-level controls first, before using the risk and control matrix, makes the risk and control matrix more efficient.

In Summary

As auditors, we need to keep in mind that Management Controls are not the same thing as Internal Controls, and that control frameworks such as COSO are necessary for consistently reporting on controls across an organization. But, COSO is not intended to replace the many management models used successfully in organizations.

Using the COSO Map

Appendix 1 - The COSO Map

Internal or Control Environment - the tone of an organization, which impacts and sets the basis for how objectives, internal controls and risks are viewed and addressed by the organization's people.

COSO Factor	Controls in Place
1.1 * Integrity and ethical values (codes of conduct, values statements, principles, ethics in dealing with others, procedures to determine ethical compliance)	
1.2 Commitment to competence (analysis of skills required, job descriptions, training and development requirements, professional development programs, mentoring and coaching programs, succession planning, employment contracts, career planning efforts)	
1.3 * 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, role in whistle- blowing procedures, reviews of financial information, clarity of governance processes)	
1.4 * Management philosophy and operating style (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; auditing, risks; consistency of messages and styles; voluntary compliance with non-required regulations; leadership in industry groups)	
1.5 Organization structure (organization charts, self-directed work teams, project teams, quality circles, focus groups, committee structures, organizational design functions, * centralized processing and controls, * shared services)	
1.6 * Assignment of authority and responsibility (limits of authority, approval processes, * controls over management overrides, delegations of authority, accountability mechanisms, responsibility matrices)	
1.7 Human resource standards (organization-wide HR 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)	

Using the COSO Map

1.8 Risk management philosophy and appetite (aggressive goal-setting, level of attention to detail, statements about risks and acceptable losses, depth of strategic and annual planning efforts; use of feasibility studies)	

Using the COSO Map

Risk Assessment - Objectives, Risks, and Responses - procedures used to establish organizational objectives and analyze relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed.

COSO Factors	Controls in Place
2.1 Entity-wide objective setting (communication to employees; consistency with Vision, Mission and Values statements, business plans, current conditions; involvement and commitment of management to objectives)	
2.2 Activity- and process-level objective setting (linkage to entity-wide objectives and strategic plans; specificity; communication to employees; consistency; SMART objectives; involvement and commitment of employees to objectives; formality of control objectives for processes; prioritization of objectives relative to entity-wide objectives)	
2.3 Identification and assessment of internal, external and fraud risks (mechanisms to identify internal and external risk events, inherent and residual risks, risks due to changing conditions, risks due to fraud: asset misappropriations, corruption, fraudulent statements; estimating likelihood and impact of potential risks; procedures to consider what could go wrong at entity- and activity-levels; formal risk management and * risk assessment processes; fraud prevention programs)	
2.4 Planned responses to risks (management decisions to accept, avoid, reduce or share risks based on cost, benefit, impact and likelihood)	

Using the COSO Map

Control Activities – policies and procedures that help ensure management’s directives and risk responses are carried out.

Note: 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.

COSO Factor	Controls in Place
3.1 Responses that reduce or share specific risks (reconciliations, physical safeguarding and access controls, comparisons, validity tests, proper forms design, insuring against losses, bonding of personnel, * policies and procedures that address significant business control and risk management practices; annual and long-term budgeting procedures, transaction and credit limits, standardized contracts, disaster recovery plans)	
3.2 Responses that prevent or detect the risk of intentional or unintentional errors (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; procedure manuals, desk manuals, instruction books and related training; help screens; segregation of incompatible duties - acquisition, custody, record keeping, and approval segregated)	

Note: Other Control Activities (below) ensure management's directives and risk responses are carried out in a more general way, and are not always associated with specific risk responses.

3.3 Actions by direct functional or activity management (approvals, authorizations, verifications defined in policies and procedures; secondary reviews)	
3.4 Analytical analyses (relating operating and financial data; investigating results; comparing different data sources; financial and competitor trend analysis)	
3.5 IT infrastructure controls (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)	
3.6 Top-level reviews of activities (Company-wide reviews and monitoring of budgets, earnings meetings, * reviews of operating results, disclosure committee)	

Using the COSO Map

activities, reviews of public reports by management, other reviews of organization functions, operations, or procedures)	
3.7 Industry- or function- or objective-specific controls (for instance, * 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)	

Using the COSO Map

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.

<p>3.8 Other management and quality initiatives are designed to help achieve business objectives. For instance ISO 9000, 10000, 14000 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.</p>	

Using the COSO Map

Information and Communication – identifying, capturing and communicating information in a timeframe and method that enables people to carry out their responsibilities.

COSO Factors	Controls in Place
<p>4.1 Mechanisms that support information flow inside the organization (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)</p>	
<p>4.2 Mechanisms that support information flow outside the organization (customer forums, external surveys, analyst meetings, external websites, external publications and newsletters, hotlines)</p>	
<p>4.3 Indicators and measurements (metrics, key performance indicators, measures and scorecards of performance, dashboards, benchmarking studies, heat maps, market share reports, competitor analysis)</p>	
<p>4.4 Style of communications (management messages about security, ethics, citizenship, policies, risks, controls, policies, objectives, strategies, VMV's; methods to avoid non-verbal communications that could under mind messages, such as body language; "shooting the messenger;" actions that speak louder than words; saying one thing and doing another; flavor-of-the-month presentations; "window dressing" efforts)</p>	

Using the COSO Map

Monitoring – assessing the operation of controls over time.

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

COSO Factors	Controls in Place
5.1 Ongoing monitoring of control components (asking questions while walking around, discussing controls with employees, talking with customers about employee conduct, informal comparisons and discussions, supervisor observations)	
5.2 Separate, periodic evaluations of control components (periodic reviews by * internal auditors, external auditors, regulators, ISO auditors, specialists; accreditation reviews; OSHA reviews; examiners; security reviews)	
5.3 Reporting and correcting deficiencies in controls (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, Enterprise Risk Management (ERM) Integrated Framework, and Internal Control over Financial Reporting (ICFR), Guidance for Smaller Public Companies*.
- If we consider all the COSO frameworks, these are the major factors to consider in designing or evaluating controls using COSO, and some items to look for in each Component of Control. Remember, this is not a Checklist, and not a substitute of knowing COSO! The controls given are just examples.

In providing management guidance for evaluating internal control over financial reporting, the SEC defined Entity-Level Controls to include those items marked with *. Later, in COSO SC, Entity-Wide Controls were defined as the Environment, Information and Communications, and Monitoring components.

Appendix 2 – Risk and Control Matrix

Internal Auditor Risk Watch Column, April 2009 Issue

The Matrix Revisited

By Larry Hubbard

A risk matrix is a commonly-used tool for documenting the analysis of objectives, risks, and responses. Typically a risk matrix focuses first on the inherent risks related to an objective — that is, all the risk events that could have an impact on achieving the objective, without regard to management's responses. The typical inherent risk matrix lists these risk events, along with a risk rating (e.g., high, medium, or low) of their potential impact and likelihood. Next, the matrix identifies management's response (i.e., controls) to each event and determines the overall adequacy of the design of controls. The central question of this assessment is, considering the risks identified and the responses management has in place to mitigate, or control, the risk events, is there a reasonable likelihood that the objectives will be achieved? Based on this assessment, auditors prepare an audit program to test the operational effectiveness of controls.

However, using a residual risk analysis approach that starts by identifying controls can make the risk matrix process more effective and efficient. In most processes and activities, identifying what already exists first is a more direct method. Plus, it is a more positive experience for auditors and managers, because the approach looks for good things first (controls) rather than bad things (risks).

Inherent Risk Matrix Shortcomings

Many auditors have used inherent risk matrices along with The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Internal Control–Integrated Framework* to evaluate the effectiveness of internal control over financial reporting as part of compliance with Section 404 of the U.S. Sarbanes-Oxley Act of 2002. For some, these matrices identify several shortcomings in the inherent risk format. For instance, it is easy to:

- Confuse risk with the absence or ineffectiveness of controls.
- Confuse impacts — the result of not achieving an objective — with risks that prevent achieving the objective.
- Go in a circle by identifying risks that are simply stated as the opposite of the objective.

Conversely, it is difficult and time-consuming to identify what could go wrong if there were no controls (inherent risk) because this is a theoretical question. In reality, there almost always are some controls in existence.

The result of these shortcomings is that people may identify areas in their inherent risk analysis that aren't truly risks that need to be dealt with. For example, in considering the business objective *safeguarding assets*, auditors may incorrectly identify the following as risks

- Not safeguarding assets (the opposite of the objective).
- Loss of assets (a result of not achieving the objective).
- Assets may not be available for use (an impact).
- The guard may not be awake (an ineffective control).
- There is no guard on duty or gates are not locked (missing controls).

After identifying these, auditors using this approach may overlook real risk events. In fact, in a

Using the COSO Map

business situation, determining real risks is difficult because there are already so many controls in place. Although the shortcomings of the traditional approach may not prevent auditors from developing an effective risk matrix, the process can take much longer and require several iterations. Moreover, the use of words such as *not*, *no*, and *lack of* can make this method appear to be a negative way to identify controls, thus potentially complicating the auditors' relationship with their clients.

Another shortcoming is confusion over the term *risk*. Although The IIA's *International Standards for the Professional Practice of Internal Auditing (Standards)* measures risk in terms of its impact and likelihood, in practice the term may be used in many ways, such as:

- When some managers ask, "What's the risk to the organization?", the term *risk* really means "potential impact."
- Some audit departments use the word *risk* when communicating audit findings, as a measure of the importance of the finding.
- Some organizations define risk management as a function performed by managers to identify and address important events that impact achieving objectives.
- In some organizations, risk assessment is either a component of internal control or enterprise risk management — per COSO's definitions — or a method audit departments use to develop an annual audit plan.

As challenging as these issues are, management's perception of the inherent risk matrix is the biggest shortcoming of this approach. Managers may think that identifying risks, without considering the controls already in place, is a purely intellectual act, akin to reinventing the wheel. They may not react well to participating in a risk assessment process that ignores what they already have in place to achieve objectives. And they may not see any benefits from re-thinking controls from that inherent risk base. These managers have a good point: Existing systems, procedures, and policies are not going away, even if the auditors want to imagine a world without them.

In today's businesses, most processes and activities are well-controlled. Sure, there are control gaps, but policies and procedures, training, good hiring practices, clear roles and responsibilities, monitoring, and information systems are commonplace in business. If those controls are not present, or if an organization does not have good managers, then risks are always going to be unacceptably high. In practice, the biggest risk for most organizations is existing controls not being executed.

The Residual Risk Format

With so many shortcomings, it is no wonder that most managers and workers, when asked to participate in a workshop to discuss inherent risks, regardless of the controls already in place, will find something else to do. However, many audit departments are finding that a simple shift in thinking, with a corresponding change in the risk matrix's format, can be much more successful. The residual risk approach begins by first identifying the controls already in place to achieve a business objective. Once this is done, risk identification focuses on what could still go wrong (WCGW), despite the existing controls. This process is intended to identify risks that are not already being addressed by existing controls. Managers and auditors then can determine whether to accept an individual risk or to establish new controls to mitigate it.

The residual risk format avoids the shortcomings of the inherent risk matrix. Identifying controls first decreases the temptation to identify ineffective controls as WCGWs. Instead, auditors will find ineffective controls when they test the operational effectiveness of the key existing controls.

Using the COSO Map

Managers also prefer the residual risk matrix because it treats them like good managers with good controls in place and focuses on what else could go wrong.

Some auditors have rejected the residual risk matrix method because it is not the approach demonstrated by COSO in its internal control framework. For example, the Evaluation Tools volume presents a risk matrix (Risk Assessment and Control Activities Worksheet) that lists inherent risks before controls. However, COSO is careful to state that such tools are only examples to demonstrate the concepts; they are not requirements or best practices, nor are they part of the framework. Another thing to remember about the COSO format is that risks and objectives are only related to the Risk Assessment and Control Activities components of that framework — the Control Environment, Information and Communication, and Monitoring components are different types of control that must be present to have an effective system of internal controls.

Other auditors believe a risk-based audit approach requires them to identify risks first. But risk-based auditing refers to how auditors select audits (annual audit planning) and the need to focus on the most important areas within an audit. In that sense, risk-based auditing may be easier to understand as “importance-based” auditing. The residual risk matrix approach is still risk-based, and there’s no requirement that auditors must identify risks first. By identifying what could still go wrong, auditors identify uncontrolled (residual) risks and responses to those events.

Finally, many auditors argue that if they don’t begin by identifying risks in the matrix, they won’t know if the right controls are in place. However, identifying controls and what could still go wrong will reveal any wrong or missing controls related to objectives and risks. In fact, many auditors who use the inherent risk matrix complete the controls or response to risks column first, and then fill in the risk column — effectively using the residual risk method.

Room For Both Formats

Experienced auditors know there is more than one way to perform an audit task, and some tools are more suited to some situations than others. Risk matrices are no different. The “Objective–Risks–Responses” format of a risk matrix, or an inherent risk analysis, is best used with high-level business objectives, such as increasing market share or maximizing revenues, where there are few specific controls or responses already in place. On the other hand, using the inherent risk matrix where many controls are already in place, leads to the shortcomings above. Because most audits are performed in established areas where systems and processes exist, the residual risk approach of identifying controls first, then asking what could still go wrong, can save audit time and lead to a more positive product.

An example Residual Risk Matrix is available in the features section of Internal Auditor’s Web site, www.internalauditoronline.org. See Below.

Larry Hubbard, CIA, CPA, CISA, CCSA, is principal of Larry Hubbard & Associates, an auditor training company based in Bethesda, Maryland.

[Online Sidebar: The Residual Risk Matrix

A risk matrix is a commonly-used tool for documenting the analysis of objectives, risks, and responses. Typically a risk matrix focuses first on the inherent risks related to an objective — that is, all the risk events that could have an impact on achieving the objective, without regard to management’s responses. The typical inherent risk matrix lists these risk events, along with a

Using the COSO Map

risk rating (e.g., high, medium, or low) of their potential impact and likelihood. Next, the matrix identifies management's response (i.e., controls) to each event and determines the overall adequacy of the design of controls. The central question of this assessment is, considering the risks identified and the responses management has in place to mitigate, or control, the risk events, is there a reasonable likelihood that the objectives will be achieved? Based on this assessment, auditors prepare an audit program to test the operational effectiveness of controls.

However, using a residual risk analysis approach that starts by identifying controls can make the risk matrix process more effective and efficient. In almost all processes and activities, identifying what already exists first is a more direct method. Plus, it is a more positive experience for auditors and managers, because the approach looks for good things first (controls) rather than bad things (risks).

Using the COSO Map

The residual risk approach starts with identifying the controls in place to achieve an objective. In this diagram, Controls 1 through 4 already exist and are identified during the audit interviewing process or self-assessment workshops. In asking “What could still go wrong” (WCGW), auditors and managers are trying to identify risks that are not already being addressed by existing controls. In this diagram, Control 5 already exists in another area and helps to mitigate Risk 1 — the auditors just did not identify it earlier. Control 6 is a new control that auditors and managers have determined needs to be implemented to mitigate Risk 2 (this may be among the “findings” of the audit). Control 2, which the auditors had already identified, mitigates Risk 3. Finally, management has decided to accept Risk 4 since this residual risk is within management’s tolerance level for that risk.

Business Objective: _____

Controls Presently in Place

- Control 1
- Control 2
- Control 3
- Control 4

What could still go wrong (WCGW)

- Risk 1
- Risk 2
- Risk 3
- Risk 4

Other Controls

Control 5 (exists now)
Control 6 (new control)
Control 2 (exists now)
Accept this risk

Using the COSO Map

A typical inherent risk matrix format is below.

Risk Matrix

Business Objective _____

Risks	Risk Rating (H,M,L)	Response to Risk	Adequacy

In this format, all important risk events that could impact achieving a business objective are listed, along with a Risk Rating (High, Medium, or Low) of the potential impact and likelihood of each event. Then, management's response to each event is identified, and the overall adequacy of the design of controls is determined. That is, how likely is the objective to be achieved, considering the risks identified and the responses management has in place to mitigate, or control, the risk events? After this evaluation of "design adequacy," auditors would prepare an audit program to test the "operational effectiveness" of controls.

End of article