Risk Assessment Checklist
Internal Controls

Introduction

The second internal control standard, as set forth by the U.S. Government Accountability Office (GAO), specifies that internal controls should provide for an assessment of the risks a governmental entity faces from both external and internal sources. A precondition to such risk assessment is the establishment of clear, consistent goals, objectives, and measurement criteria at both the entity-wide and activity or program level, as applicable.

Goals, or long-term objectives, should be established based on applicable State and federal laws and regulations, considering the priorities of the Governor and entity management. Also, the goals and objectives should be consistent with the entity's Mission Statement which should also be based on applicable laws. After the goals have been determined, the entity determines to what extent short-term objectives are required to achieve the long-range goals at both the entity-wide and activity or program level. Then, the entity identifies the risks that could prevent or impede the achievement of the goals and objectives at each respective level. Management then determines an approach for ongoing risk-assessment management and the internal-control activities necessary to mitigate risks in order that achievement of the internal control objectives of efficient and effective operations, reliable financial reporting, and compliance with federal and State laws and regulations can take place.

Implicit in management's approach to risk assessment are the following steps or phases:

- Identifying internal and external events and risks affecting achievement of the entity's goals and objectives.
- Analyzing and assessing the risks, considering the likelihood and impact (cost/benefit). A rating scale of high/medium/low or high/low is adequate.
- Establishing internal controls to achieve the risk responses.
- Allocating resources to those areas of risk where the combination of risk likelihood and impact will sustain the greatest negative consequences for the entity.

The matrix below illustrates the possible combinations.

Risk Likelihood (in Italics)	**Risk Impact (in Bold)**		
	High / **High**	*High* / **Medium**	*High* / **Low**
	Medium / **High**	*Medium* / **Medium**	*Medium* / **Low**
	Low / **High**	*Low* / **Medium**	*Low* / **Low**

Outlined below is a list of questions covering control objectives for risk assessment that an entity might consider. This list is merely a beginning point. It is not all-inclusive, nor will every item apply to every governmental entity, or activity or program within an entity. Although some of the functions and points may be subjective in nature and require the use of judgment, they are important in performing risk assessment. Risk identification and assessment responsibilities are a responsibility/function of entity management; however, some agencies delegate some of these responsibilities to their internal auditors.

Benefits of Adopting the COSO Model

COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. COSO is jointly sponsored by the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the Institute of Internal Auditors, and the Institute of Management Accountants.

As COSO guidelines suggest, applying the COSO Framework/Model is a fairly intuitive process. Quite often, organizations are already doing this type of analysis, but may not realize it. By formally adopting the COSO model, or at least putting a COSO-like environment in place, organizations have guideposts to follow. These guideposts can help management identify, structure, and implement changes that may seem overwhelming at first. COSO can also help reduce errors and increase efficiencies, as well as anticipate problems and provide guidance on how to respond. Moreover, it allows management and auditors to speak a common language. Finally, having internal controls correlate with the Framework's guidelines can help streamline the auditing process, and that may even lower audit costs to a degree.

Overall, the Framework has held up very well. COSO has issued other guidance on enterprise risk management (ERM or COSO II) and has clarified various aspects of the Framework. Yet the core principles have not changed. In fact, they have only been reinforced by subsequent publications. COSO seems to understand that business operations have changed greatly since COSO was first issued, especially in the area of information technology, and its subsequent publications reflect this.

Control Goals and Objectives Questions:

A.	Establishment of Entity-Wide Goals and Objectives:	Yes	No	N/A	Comments
1.	Has management established an overall entity-wide mission statement which is consistent with federal and State laws?				
2.	Has management established overall entity-wide goals/long-term objectives based on applicable State and federal laws and regulations?				
3.	Are the entity-wide goals/long-term objectives specific enough to apply to the entity itself apart from all other governmental entities or agencies?				
4.	Have entity-wide goals/long-term objectives been clearly communicated to all employees?				
5.	Has management received feedback indicating that communication to employees regarding entity-wide objectives is effective?				
6.	Do the entity's strategic operating plans support the entity-wide goals/long-term objectives?				
7.	Do the entity's strategic operating plans address resource allocations and priorities?				
8.	Are strategic plans and budgets designed with an appropriate level of detail for various management levels?				
9.	Does the entity have an integrated management strategy and risk assessment plan that considers the entity-wide goals/long-term objectives and relevant sources of risk from internal management factors and external sources?				
10.	Has an adequate internal control structure been established to address risks from internal management factors and external sources?				

B.	Establishment of Activity-Level Objectives:	Yes	No	N/A	Comments
11.	Do activity-level (or program-level) objectives support the entity's entity-wide goals/long-term objectives and strategic plan?				
12.	Are activity-level objectives reviewed periodically to assure that they have continued relevance?				
13.	Are activity-level objectives complementary to and reinforce all other such level objectives, and not contradictory?				
14.	Have objectives been established for all key operational and support activities relative to the activity or program?				
15.	Are activity-level objectives consistent with effective past performances and best business practices that may apply to the entity's operations?				
16.	Are allocated entity resources adequate relative to the activity-level objectives?				
17.	Has management identified those activity-level objectives that are critical to the success of the overall entity-wide objectives?				
18.	Do critical activity-level objectives receive appropriate attention and review from management?				
19.	Is the performance on critical activity-level objectives monitored on a regular basis?				
20.	Are appropriate levels of management involved in establishing the activity-level objectives and committed to their achievement?				
21.	Are measurement criteria, for both entity-wide and program level, used in assessing whether objectives are achieved over time?				
22.	Are the performance measures used in management decision making?				

C.	Risk Identification:	Yes	No	N/A	Comments
23.	Is identifying and documenting internal and external events and risks affecting achievement of the entity's goals/long-term objectives incorporated into management's short-term and long-term forecasting and strategic plan (risk identification)?				
24.	Does the risk identification process include identifying the entity's key internal process strengths and weaknesses and key external threats and opportunities (brain-storming activity)?				
25.	Has the entity prioritized the opportunity and threat outcomes by high and low impact and high and low likelihood?				
	Is the risk identification process updated at least annually, considering each of the following:				
26.	Findings from internal and external audits, evaluations, and other types of assessment activities?				
27.	Factors external to the entity?				
28.	Risks inherent with technological advancements and developments?				
29.	New laws and regulations?				

C.	Risk Identification:	Yes	No	N/A	Comments
30.	Business, political, and economic changes?				
31.	Major suppliers and contractors?				
32.	Internal factors?				
33.	Any business process reengineering efforts or redesigned operating processes?				
34.	Highly decentralized program operations?				
35.	Major changes in the entity's managerial responsibilities?				
36.	Certain human capital related risks, such as the inability of the entity to provide for succession planning or to retain key personnel due to the inadequacy of the entity's compensation and benefit programs in competition with the private sector?				
37.	Availability of future funding for new programs or the continuation of current programs?				
38.	Previous failures to attain the entity's missions, goals, objectives, or to stay with budget limitations?				
39.	The nature of the entity's mission or the significance and complexity of any specific related programs or activities?				
40.	Is the corrective action status (i.e. implemented, partially implemented, not implemented) of all internal and external audit findings and recommendations tracked and reported to management?				
41.	Does the entity evaluate and reconsider the high-impact outcomes and start the process over again?				

D.	Risk Analysis and Assessment:	Yes	No	N/A	Comments
42.	Has management established a formal, written process to analyze and assess risks, and is the process completed/updated at least annually?				
43.	Have criteria been determined for categorizing risks as low, medium, and high risks?				
44.	Are risks identified and analyzed relative to the entity's overall mission, goals, and objectives as well as corresponding activity/program objectives?				
45.	Does the entity's risk analysis include assessing the likelihood, frequency, and impact of each identified risk event and assigning a risk category (high, medium, low) to each event?				
46.	Has management developed an approach for risk management and control based on the amount of risk that can be prudently tolerated considering the costs versus the benefits of reducing the risk?				
47.	Are specific control activities in place to manage or mitigate risks both entity-wide and at each activity/program level?				

D.	Risk Analysis and Assessment:	Yes	No	N/A	Comments
48.	Does the entity's risk assessment process include selecting risk responses [(a) acceptance of risk {retain, budget for}, (b) avoidance of risk {eliminate, withdraw from, or not become involved}, (c) sharing {transfer, outsource, or insure}, or (d) reduction {optimize, mitigate}] for each identified risk? [Though this step in the Risk Assessment process is part of COSO II, not COSO I, it is highly effective in assisting entity management in managing their identified risks.]				
49.	Does the entity's risk assessment process include developing and/or strengthening internal controls as necessary to reduce each identified risk to an acceptable level?				
50.	Does the entity's risk assessment process include allocating resources to those areas of risk where the combination of risk likelihood and impact will sustain the greatest negative consequences for the entity?				
51.	Are the implementation and operation of controls appropriately monitored?				
52.	Does the entity's risk assessment process include developing a set of actions, including strengthening internal controls, for identified risks to align those risks with the entity's risk tolerance and risk appetite?				
53.	Has the entity established internal controls for high-impact threat outcomes with a high likelihood of occurrence?				
54.	Does the entity focus and manage efforts and resources to produce and achieve high-impact opportunity outcomes and reduce or minimize high-impact threat outcomes?				

E.	Managing Risk During Change:	Yes	No	N/A	Comments
55.	Does the entity have mechanisms in place to anticipate, identify, and react to risks presented by changes in governmental, economic, industry, regulatory, operating, or other conditions that can affect the achievement of entity-wide and activity/program goals and objectives?				
56.	Are routine changes addressed adequately through the established risk identification and analysis/assessment processes?				
57.	Is management attentive to risks resulting from the hiring of new personnel in key positions or by high personnel turnover in a particular area?				
58.	Do adequate mechanisms exist to assess risks posed by the introduction of new or changed information systems and also the risks involved in training employees to use the new systems?				
59.	Does management give appropriate consideration to the risks inherent with rapid growth and expansion or rapid downsizing and its impact on system capabilities?				

E.	Managing Risk During Change:	Yes	No	N/A	Comments
60.	Does management give appropriate consideration to the risks involved when introducing major new technological developments and applications and also when incorporating them into the entity's operating processes?				
61.	Are risks sufficiently analyzed at times when the entity begins the production or provision of new outputs and services?				