COMMENT SHEET

Comment #	Page # (#25)	Section #	Recommendation/Revision (NASA)	Rationale
1	1	Foreword	Modify 1st sentence to after program manager to include "and other Agency officials involved in the management and oversight of Agency programs and operations"	There are other stakeholders affected by Internal Controls that should be mentioned in this section.
2	1	Foreword	Modify 2nd paragraph, 2nd sentence to add: "These standards, published by the Government Accountability Office (GAO), are known as . . . (Green Book), which provide . . . ."	GAO should be cited in the Foreword for its ownership of the standards even though the revision of the Green Book was performed by a variety of organizations from government, industry, and academia.
3	5	2.02	Change the 3rd sentence in this paragraph to read "In implementing the Green Book, management should (or must) design the policies…"	This should be a requirement clearly stated up front.
4	5	2.03	On the second sentence of this paragraph change "…entity's oversight body, may set objectives" to "…entity's oversight body, should set objectives"	Doesn't any organization expected to have objectives in order to efficiency and effectively run their operations?
5	6	2.04	To the first sentence on the fourth bullet add "of" "The quality of information…"	Grammatical fix
6	8	2.09	Under Control activities, 10. "Management should design control activities to achieve objectives and risk responses." change to "and responses to risk".	Better use of the term.
7	9 and other pages that illustrate COSO cube	2.1	Instead of repeating the COSO cube throughout the document, use it once along with a government hybrid to replace Function - Entity level. Recommend consideration of Hierarchy as Oversight body; Management; Entity level; Staff. These levels are more consistent with the overall revisions to the Green Book.	The government references are aimed at being consistent with the overall revisions to the Green Book. They also clarify the terminology most used for levels of organizations - illustration format would be helpful.

Comment #	Page #	Section #	Recommendation/Revision	Rationale
8	10	2.16	On the third sentence of this paragraph replace "Management may include setting objectives…" with Management should include setting objectives".	Setting objectives in an organization should be something that is required in order to establish an adequate internal control system.
9	10	2.17	Consider replacing 2nd reference to "management" with "the entity".	Usage of "the entity" is logical level.
10	10	2.18	The first sentence should state that "Management groups objectives into each of the three categories of objectives"	Entities should have the 3 objectives (operations, reporting, and compliance) and have not the option of selecting one of these.
11	12	2.24	There should be a definition of "Assets" somewhere before this section.	To help users understand what exactly is an asset.
12	12	2.25	On the title of the setting please add a hyphen between Sub and Objectives (should read Setting Sub-Objectives)	Grammatical correction
13	14	3.06	On the last sentence of the paragraph, the concept "necessary authority or competence to perform the control effectively" should be explained.	Concept not clear. Would help reader if it is clarified.
14	22	1.12	On the 4th sentence it would help to add the word "should" when talking about addressing deviations by management "Management should…."	This should be a requirement clearly stated.
15	24	2.07	On the second sentence consider removing OMB given that they are part of the White House and it sounds repetitive.	To make message clearer.
16	25	2.11 and 2.12	Through the Green Book some sections sound like requirement and other as descriptions. For example, on these section 2.11 uses the word "should" (making it sound like a requirement) and 2.12 does not (The oversight body oversees (sounds descriptive). Suggest changing for consistency.	To make requirements and discussion consistent.
17	37	6.12	Suggest clarifying concept more and adding more description to the first bullet.	First bullet is very important and lacks more information about this type of risk tolerance.

Comment #	Page #	Section #	Recommendation/Revision	Rationale
18	38	7.05	The terms "residual risk" and "inherent" risk" should be better defined. Suggest using the following definitions: **Residual:** A risk that remains after all efforts have been made to mitigate or eliminate risks associated with a business process. After a risk assessment, a residual risk may be known but not completely controllable, or, it may not be known. In either case, the residual risk is assumed by whoever owns the business process. **Inherent** A risk of misstatement due to error or fraud that may exist within a financial statement regardless of management's awareness of the error. An assessment of inherent risk can be based on a number of factors, including difficulties in calculating precise valuations, or uncertainties in the current environment.	To explain the concepts of risks in a clearer manner.
19	40	7.12	Replace "Acceptance - No action is taken to respond to the risk" by "Acceptance -Action is taken to respond to the risk by accepting the risk as is.	
20	40	7.12	Replace "Reduction - Action is taken to reduce the likelihood or magnitude of the risk" by "Reduction - Action is taken to reduce the likelihood and/or impact of the risk	
21	41	8.04	Add the following sentence before the first sentence of the paragraph "During the Internal Control reporting process any instances of fraud, waste and abuse should be communicated to officials responsible for the Agency's Internal Controls".	Communicating internal controls to stakeholders responsible for Internal Controls will help increase visibility of the problems in order for internal controls' officials for implementing internal controls to prevent the problem from arising in the future.
22	43	9.01, 9.05	Give guidelines or criteria for Significant changes	If you don't give clear guidelines then it is subject to interpretation which creates problems within the organization
23	43	9.03,9.04	Give guidelines or criteria for …"Significantly impact…"	If you don't give clear guidelines then it is subject to interpretation which creates problems within the organization
24	47	10.06	Add "Program Reviews" in the box.	Program reviews should stand out from the other categories, especially because program managers often think they are exempt from internal control activities.
25	60-67	13	The section needs more description and examples.	The Information and Communication section needs to provide more guidance. This section was not adequately done in the previous Green Book.

Comment #	Page #	Section #	Recommendation/Revision	Rationale
26	70	16.08	Change the last sentence to : "Ongoing monitoring . . .electronically capturing evaluations of controls and transactions."	The tools don't evaluate.
27	74	New 17.11	Title should be "Validate Completion of Corrective Actions". Move last sentence in 17.10 to 17.11.	This change gives closure to the cycle of creating corrective actions, monitoring, completing, and finally verifying/validating that the corrections have actually been done according to requirements.
28	75	Terms	Add to "Application control activities" the words "integrity and quality" before "confidentiality". Change "Contingency plans" to replace "personnel" with "control environment".	Should not omit integrity and quality from this list of controls. The change of personnel to control environment is much broader a term to use with reference to contingency planning.
29	76	New term needed	Add "Entity" to the definitions. It is used so often in the Book but never defined. Perhaps: An organizational unit such as a program or function responsible for carrying out activities and achieving objectives.	Entity is a key word in the document. Oversight bodies and Management are defined, but not entity.
30	78	Security Management	Add: "The information and workforce processes and control activities related to access rights in an entity's information technology and staff."	Should consider personnel security as well as IT.
31	Thorough document	Authoritative Guidance	Thorough the document there is a lack of authoritative guidance that helps the reader understand where the requirements are coming from. For example, on page 10 (section 2.17) a reference to FFMIA would help understand that this requirement derives from another authority.	To help the reader better understand the concepts.

Page 10

02.16 – Isn't this a requirement under FMFIA? Should there be references in this document for these types of things to support understanding?

Page 11

Operations Objectives

O2.19 Operations objectives relate to program operations that achieve an entity's mission. An entity's mission may be defined in a strategic plan. Such plans set the goals and objectives for an entity along with the effective and efficient operations necessary to fulfill those objectives. Effective operations produce the intended results from operational processes while efficient operations do so in a manner that minimizes the waste of resources.

O2.20 Management can set, from the objectives, related sub-objectives for units within the organizational structure. Management, by linking objectives throughout the entity to the mission, improves the effectiveness and efficiency of program operations in achieving the mission.

Definitions not clear – see discussion, also, on "assets/resources" below.

The concept of "operations" may still remain the greatest challenge area in terminology and ambiguity, although the language indicates financial and non-financial (e.g. reporting). COSO has stated that *Efficiency and effectiveness in operations* – "addresses an entity's basic business objectives, including performance goals and safeguarding of resources." When looking at any one category--the effectiveness and efficiency of operations, for instance--all five components must be present and functioning effectively to conclude that internal control over operations is effective. Agreed, but what is a business objective meant to be in the absence of the achievement of business mission. For Federal Government, the achievement of business mission is reflected by both its founding legislation and its appropriations. These tell us what our primary goals are and compliance both programmatically and financially starts here. There is no reflection or suggestion that the budget is part of the internal control framework, and yet there is much discussion in the GAO document about performance and accountability. There are important linkages there. The GAO Internal Control Management and Evaluation Tool (GAO-01-1008G) contains some relevant and important language that would be useful to include in this topic area and may be worth reiterating here. From Page 23 headed by Establishment of Entity-wide Objectives through to the following gives clear guidance in the integration of internal controls activities and helps in establishing an understanding around objectives. Is this then the "business objectives", or something else? Also are programmatic controls (ensuring program goals are achieved) meant to specifically be a business objective or not?:

There is a relationship and consistency between the agency's operational strategies and the entity-wide objectives. Consider the following:
. Strategic plans support the entity-wide objectives.
. Strategic plans address resource allocations and priorities.
. Strategic plans and budgets are designed with an appropriate level of detail for various management levels.
. Assumptions made in strategic plans and budgets are consistent with the agency's historical experience and current circumstances.

4. The agency has an integrated management strategy and risk assessment plan that considers the entity-wide objectives and relevant sources of risk from internal management factors and external sources and establishes a control structure to address those risks. This, however, suggests that Enterprise Risk Management is appropriate here but others are saying internal controls are not part of this equation, so which is it? Again the language is not clear, and is causing some confusion. Granted internal controls must be reasonable and it is not meant to guarantee success, but if it is seen only as a financial objective then the interconnectivity between money and program may remain disconnected. If this were not the case would GAO still find that "*While federal grant funding has been increasing, long-standing concerns remain about the federal government's grants management and the lack of effective oversight tools to reasonably assure that grants are used for their intended purposes and that risks of fraud, waste, and abuse are minimized. GAO has issued a range of reports raising concerns about the risks and vulnerabilities related to grants management and oversight.*"

Establishment of Activity-Level Objectives Comments/Descriptions
1. Activity-level (program or mission-level) objectives flow from and are linked with the agency's entity-wide objectives and strategic plans. Consider the following:
. All significant activities are adequately linked to the entity-wide objectives and strategic plans.
. Activity-level objectives are reviewed periodically to assure that they have continued relevance.
2. Activity-level objectives are complementary, reinforce each other, and are not contradictory.
3. The activity-level objectives are relevant to all significant agency processes. Consider the following:
. Objectives have been established for all the key operational activities and the support activities.
. Activity-level objectives are consistent with effective past practices and performance, and are consistent with any industry or business norms that may be applicable to the agency's operations.
4. Activity-level objectives include measurement criteria.
5. Agency resources are adequate relative to the activity level objectives. Consider the following:
. The resources needed to meet the objectives have been identified.
. If adequate resources are not available, management has plans to acquire them.
6. Management has identified those activity-level objectives that are critical to the success of the overall entity-wide objectives. Consider the following:
. Management has identified the things that must occur or happen if the entity-wide objectives are to be met.
. The critical activity-level objectives receive particular attention and review from management and their performance is monitored regularly.
7. All levels of management are involved in establishing the activity-level objectives and are committed to their achievement.

Page 11, continued

O2.21 Reporting objectives relate to the preparation of reports for use by the entity, its stakeholders, or other external parties. Reporting objectives may be grouped further into subcategories:

- External Financial Reporting Objectives - Objectives related to the release of the entity's financial performance in accordance with professional standards, applicable laws and regulations, as well as expectations of stakeholders. Shouldn't this make some sort of comment about it's or conformance or relevance to accounting theory, standards, and requirements more specifically? If this were clearer perhaps Agencies would not fail to recognize things like environmental liabilities that go unrecorded. Many seem not to recognize that receivables include some aspect of the results of A-133 and OIG audit findings and other oversight management activities that identify funds that should be returned to the government (how much is really out there in unrecorded receivables)? Why is Federal financial management so different that this is not an important reflection of the Balance Sheet?
- External Nonfinancial Reporting Objectives - Objectives related to the release of nonfinancial information in accordance with professional standards, applicable laws and regulations, as well as expectations of stakeholders.
- Internal Financial Reporting Objectives and Nonfinancial Reporting Objectives - Objectives related to gathering information needed by management to support decision making and evaluation of the entity's performance.

Page 12

Should the discussion of objectives ask the question?:

Are objectives defined to meet the entity's mission, and its unit operational and functional requirements, and compliance or conformance with applicable laws and regulations, strategic plan, and other goals, initially and annually updated? In other words, as part of designing the entity internal control system, has management defined the objectives in specific and measureable terms to enable it, its functional units and operations, and its members to identify, analyze, and respond to risks related to achieving those objectives?

Categories of Objectives

Objectives would fall into one or more of the three categories of objectives: Don't they really translate to all 3, if fully integrated? Compliance, for instance shows up across the board whether programmatic or financial from appropriations language to OMB Circulars, to regulatory language.

Operations - Effectiveness and efficiency of operations

Reporting - Reliability of reporting for internal and external use

Compliance - Compliance with applicable laws and regulations

Safeguarding of Assets – The placement of this section is either rather arbitrary or there should be an expansion of the expression of the ideas here

A subset of the three categories of objectives is the safeguarding of assets. Management designs an internal control system to provide reasonable assurance regarding prevention or prompt detection of unauthorized acquisition, use, or disposition of an entity's assets. Assets include people, money and inventory. Inventory can further be defined by property, plant, equipment, information, supplies, goods, and services. So for instance, lack of access to needed goods and services through acquisitions or as a result of weaknesses in quality controls can impede or cause risk even to life or to mission objectives. A shortage of people can impact compliance objectives (no one there to fulfill the requirement or to ensure the oversight of programs. Non-compliance with hiring laws and requirements such as Equal Opportunity can give rise to Agency liabilities. A limited grants applicant pool, unless intended, can impede opportunities and create risk in mission objectives. Information is considered an asset and if it is vulnerable or incomplete or inaccurate it can create Agency risk and may be a reflection of an internal control weakness. Without a more complete picture of what we are ensuring our controls will assert we may continue to have weak control frameworks.

Setting Sub-objectives

Management can develop from objectives more specific sub-objectives throughout the organizational structure. Management needs to define sub-objectives in specific and measurable terms that can be communicated to the personnel who are assigned responsibility to achieve these sub-objectives. Both management and personnel require an understanding of an objective, its sub-objectives, and defined levels of performance to ensure accountability in an internal control system. This is true, however, if the message is that internal controls are financial and about the processes that support financial activity then it will likely not translate to the other kinds of risks identified in the previous paragraph for an integrated, efficient, and effective framework.

What is important in each category is recognizing entity and Agency risk to its objectives and its mission in order to evaluate the extent or reasonableness of the controls, and the objective setting process.

How is the internal control system defined? Are there no basic tenants for what constitutes this system? There are several references to it in the document, but it does not seem to define it. So if there is not clear definition, then it becomes difficult to evaluate, report on, and explain from an internal controls perspective.

No two entities will have an identical internal control system due to differences in factors such as mission, regulatory environment, strategic plan, entity size, risk tolerance, and information technology. ***Page 9***
The Green Book, however, does not prescribe the process for how management designs, implements, and operates its internal control system. ***Page 7***
In general, all components, principles, and attributes are relevant for an effective internal control system. However, there may be an operating or regulatory situation in which management has determined that a principle or attribute is not relevant for the entity to achieve its objectives and address related risks. Relevance refers to management's determination that each principle and attribute has a significant bearing on the design, implementation, and operation of its associated component. ***Page 7***

An effective internal control system provides reasonable assurance that the organization will achieve its objectives. It requires that

• each of the five components, 17 principles, and relevant attributes of internal control are effectively designed, implemented, and operating and

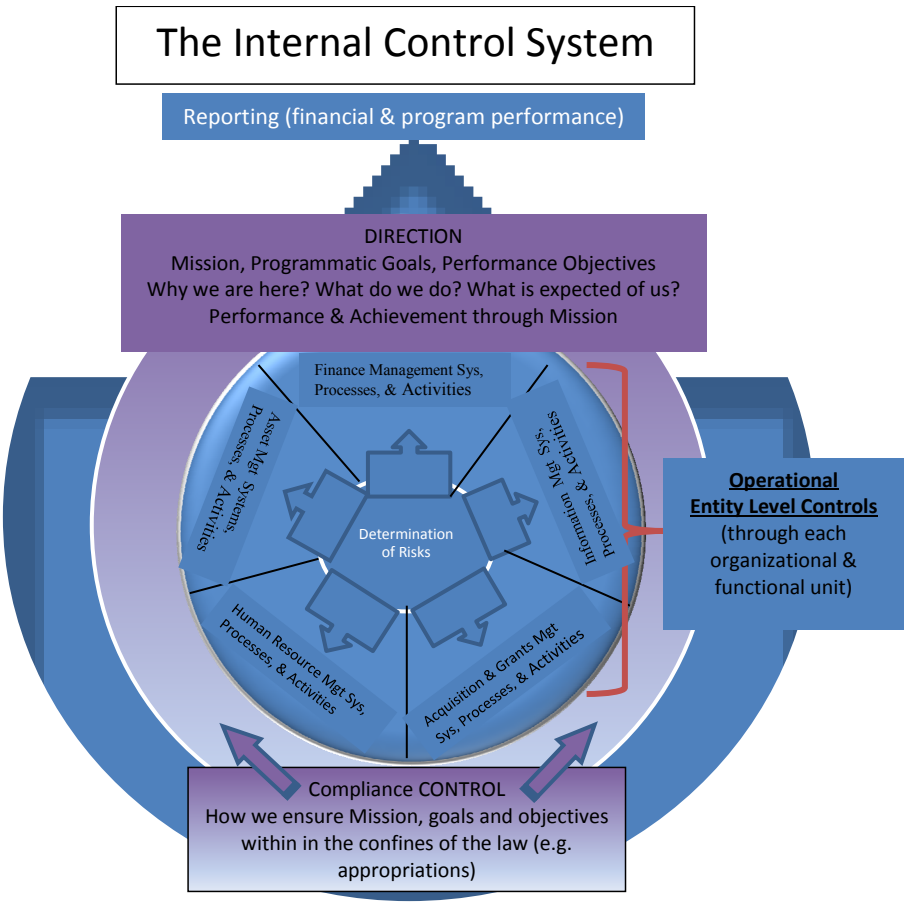
• the five components are operating together in an integrated manner.

O3.02 To determine if an internal control system meets these requirements, management evaluates the effect of internal control deficiencies on the internal control system. ***Page 13***

Perhaps a simple language summary would help, like:

Internal Controls are to be an integral part of any organization's financial and business policies and procedures. Internal controls consists of all the measures taken by the organization for the purpose of; (1) protecting its resources against waste, fraud, and inefficiency; (2) ensuring accuracy and reliability in accounting and operating data; (3) securing compliance with the policies of the organization; and (4) evaluating the level of performance in all organizational units of the organization. Internal controls are simply good business practices.

Or perhaps a picture . . .:



The systems identified in the picture are cross-cutting – the pillars, so to speak, to the "internal control framework" in this case. All programs and all operational activities move through these same systems and activities, no matter what your organization, big or small. Safety issues and related compliance requirements can cut across each, and are both programmatic and financial. We have certain goals and objectives, like safety, that aren't necessarily understood in this framework. Aren't there key attributes no matter which or what size the organization that should be basic tenants or themes that are includable or must haves for everyone? I think people would like to know what these might be.

If you could bring the sample picture, above, up a little it would be that the programs are supported through each of these systems (the funds and the assets, and other resources flow through the middle of each program). If you could carve out a side view you should see all the organizational functional and operational units. We are responsible and accountable to the public to fulfilling the social objectives that each Agency is tasked with. How we perform flows through our mission and would be reported out through the top. Evaluating risk is at the core and is evaluated through each component part of the structure. But perhaps this is an over-reflection of an internal controls system. Again, I think folks are looking for some clearer guidance in moving beyond financial in the Federal arena.

The *Questions for Commenters* asks, " *Does the framework provide the necessary information to allow program managers to evaluate the internal controls for their programs?".* If I were in charge of a grant program, I would say "not likely", because I do not see the connection or enough explanation for programs. If I were a program manager in a mission support directorate (in charge of infrastructure, acquisitions and grants, and even safety, I would understand to a degree, but figure the finance people handle most if not all of this. They look at our transactions and tell us when they find something we need to fix and the auditors also let us know when we need to address something. We are very responsive to the auditors.

Page 17 (Wouldn't hurt to reiterate as indicated below for each of the five):

The Green Book has specified documentation requirements in five attributes in the framework, with discussion of these requirements in the accompanying application material. These are:

- Principle 3: Paragraph 3.12

Management should develop and maintain documentation of its internal control system.

- Principle 12: Paragraph 12.03

Management should document in policies the internal control responsibilities of the organization.

Principle 16: Paragraph 16.12

Management should evaluate and document the results of ongoing monitoring and separate evaluations to identify internal control issues.

- Principle 17: Paragraph 17.07

Management should evaluate and document internal control issues and determine appropriate corrective actions for internal control deficiencies on a timely basis.

- Principle 17: Paragraph 17.09

Management should complete and document corrective actions to remediate internal control deficiencies on a timely basis.

Page 21

Since this GAO document is COSO translated to Government, shouldn't Standards of Conduct make some reference to roles and responsibilities as a Public Servant. In the U.S., Code of Ethics--adopted on July 11, 1958--should be adhered to by all government employees and public servants, which translates into efforts and activities around internal controls responsibilities and obligations. Perhaps it is the elephant in the room, but it wouldn't hurt. Need more authoritative references.