1. Is the hierarchy of components, principles, and attributes clearly explained?

- **Section 1 - Fundamental Concepts of Internal Control**

Definition of Internal Control

O1.03 Internal control comprises the ***strategic*** plan(s), methods (preventive and detective), policies, ***monitoring*** and procedures ~~used to fulfill the mission, strategic plan, goals, and objectives~~ of the organization. ~~Internal control serves as the first line of defense in safeguarding assets. In short, internal control helps federal managers achieve desired results through effective stewardship of public resources.~~

*Comment - The use of the term strategic plan incorporates vision, mission, values, goals and objectives, action plan for each objective and reporting. Last sentence would be part of a goal. See page 20 on Principle 1 - Demonstrate Commitment to Integrity and Ethical Values (**1.04**).*

Adding the two methods of internal control into Control Environment will enhance the readers understanding. There may be more to methods than just the two mentioned below.

Note. As a former Internal Control Manager at the third highest level for multiple programs we had to sign a Standards of Conduct in order to manage funds and resources. Also, instructed Strategic Planning and thus I feel confident it the state on the use of the term.

1. **Preventative Controls**: that are designed to discourage errors or irregularities from occurring (ie., processing vouchers only after signatures have been obtained from appropriate personnel)
2. **Detective Controls**: that are designed to find errors or irregularities after they have occurred (ie., reviewing departmental phone bills for personal calls).

---------- next question follows ----------

5. Are the requirements for management to design, implement, and operate an internal control system clear, understandable, and adequate?

- **Section 2 - Establishing an Effective Internal Control System**

Components, Principles, and Attributes

O2.03 An entity ~~determines its mission, sets~~ ***publishes*** a strategic plan, which includes objectives, and formulates ***action*** plans to achieve its objectives. ~~Management, with oversight from the entity's oversight body, may set objectives for an entity as a whole, or may target activities within the entity which may include monitoring.~~ Comment – this sentence is found in **Roles in an Internal Control System (page 9)** and policy**.**

Page 11 at the top. A simple technique would be as shown below and thus elimination of what was previously written on page 4. Could continue this technique with reporting and compliance objectives.

Operations Objectives - Effectiveness and efficiency of operations

O2.19 Operations objectives relate to program operations that achieve an entity's mission….

---------- next question follows ----------

7. Are the roles, divisions, and overlaps of responsibility for the oversight body, management, and personnel clear, understandable, and adequate?

- **Section 4 - Additional Considerations**

Documentation

O4.08 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 Document Internal Control System

Principle 12: Paragraph 12.03 Document Responsibilities through Policies

Principle 16: Paragraph 16.12 Perform Monitoring Activities

Principle 17: Paragraph 17.07 Evaluate Issues

Principle 17: Paragraph 17.09 Complete Corrective Actions

Note – Easier for the reader to see the quick bullet comment then page back and forth through the Green book.

Risk Assessment

Page 37

6.12 Management defines risk tolerances in specific and measurable terms so they are clearly stated and can be measured. Risk tolerance is often measured in the same unit as the performance measures for the defined objectives. Depending on the category of objectives, risk tolerances may be expressed as follows:

• Operations and Compliance Objectives - Acceptable level of variation in performance in relation to risk.

• Nonfinancial Reporting Objectives - Required level of precision and accuracy suitable for user needs.

• Financial Reporting Objectives - Material misstatements, including omissions, are those that, either individually or in the aggregate, could reasonably be expected to influence the decisions of financial statement users. Judgments about materiality are made in light of surrounding circumstances, involve both qualitative and quantitative considerations, and are affected by the needs of financial statement users and size or nature of a misstatement.

Comment – Risk tolerance is not clear nor are is there any guidance on the rating. Recommend inserting the following for clear and understandable for the reader.

Risk assessment provides a mechanism for identifying which risks represent opportunities and which represent potential pitfalls. Done right, a risk assessment gives organizations a clear view of variables to which they may be exposed, whether internal or external, retrospective or forward-looking. A good assessment is anchored in the organization's defined risk tolerance, and provides a basis for determining risk responses. Risk rating scales may be defined in quantitative and/or qualitative terms. Quantitative rating scales bring a greater degree of precision and measurability to the risk assessment process. However, qualitative terms need to be used when risks do not lend themselves to quantification, when credible data is not available, or when obtaining and analyzing data is not cost-effective.

Organizations typically use ordinal, internal, and/or ratio scales. Ordinal scales define a rank order of importance (e.g., low, medium, or high), interval scales have numerically equal distance (e.g., 1 equals lowest and 3 equals highest, but the highest is not 3 times greater than the lowest), and ratio scales have a "true zero" allowing for greater measurability (e.g., a ranking of 10 is 5 times greater than a ranking of 2). Risk rating scales are not one-size-fits-all and should be defined as appropriate to enable a meaningful evaluation and prioritization of the risks identified and facilitate dialog to determine how to allocate resources within the organization.

Add risk assessment definition - Risk assessment is a systematic process for identifying and evaluating events (i.e., possible risks and opportunities) that could affect the achievement of objectives, positively or negatively. **See Principle 7 – 9 (Indentify, Analyze and Respond)**

The chart below came from page 59. QUESTION – How does a policy describe competency of internal control managers? Most organizations do not train internal managers on acceptable levels of competency to perform a control activity. Is this best suited for training and evaluation rather than in this section? Document Responsibilities through Policies

Elements of a written policy may include:

- **Timeliness** – Management documents when a control activity and any follow-up corrective actions are performed.

- **Corrective actions** – Management documents the need for appropriate follow-up when matters are identified that require investigation, and establishes responsibility for any corrective actions taken.

- **Competence** – Management documents the level of competency required to perform a control activity. Requirements depend on factors such as the complexity of the control activity and the complexity and volume of the underlying transactions.

Better to describe elements of a good written policies

• Policies are written in clear, concise, simple language.

• Policy statements address what is the rule rather than how to implement the rule.

• Policy statements are readily available and their authority is clear.

• Designated “policy experts” (identified in each document) are readily available to interpret policies and resolve problems.

• As a body, they represent a consistent, logical framework for internal control activities

• The policy counts for little unless it is implemented!