

[REDACTED]

---

**From:** Juengst, Phillip [REDACTED]  
**Sent:** Tuesday, February 18, 2014 8:02 PM  
**To:** GreenBook  
**Cc:** Blot, William; Safranek, Ellen  
**Subject:** Dept of Education/FSA comments on draft Green Book

GAO,

Below are comments on the exposure draft compiled by our Federal Student Aid office. If you have any questions, please don't hesitate to call or email me.

Thank you for the opportunity to comment.

Phillip Juengst  
Director, Financial Improvement and Post Audit Operations  
Office of the Chief Financial Officer  
[REDACTED]

General –

This Exposure Draft (ED) defines internal control requirements at a more granular level compared to existing standards and COSO. Specifically, below the standards level, the ED introduces principles (17) and attributes (48) and, for each attribute, various elements. Please be advised that this hierarchy results in significant new or expanded control requirements and may result in a dramatic increase in the level of effort for agencies to comply. It would help agencies manage workload if GAO would consider scaling back the requirements to the standard level only. Alternatively, would GAO (in coordination with OMB) consider phasing in over several years the effective dates for implementation of lower level requirements?

This ED includes significant new documentation requirements. (See pg. 17, Para. O4.08; pg. 6, Para. O2.06.) Would GAO consider phasing in adoption over time?

Please clarify your intent with respect to oversight bodies. For A-123A governance, many agencies established Senior Management Council / Senior Assessment Team structures comprised of management staff with, potentially, OIG staff participating in an advisory capacity. It wasn't clear from the existing text if this same structure would be sufficient to meet the relevant standards, principles, and attributes.

Use of the term "quality info." is redundant. Please consider defining once what the requisite attributes for information are (i.e., what is quality) and then simply referring to info. as opposed to quality info.

Section specific –

Pg. 11, Para. 02.19 – There is an inherent assumption in the reference to strategic plans that such plans describe the effective and efficient operations necessary to achieve stated objectives. This may be faulty assumption. Strategic plans may emphasize new priorities, initiatives, and investments over the established "keep the trains running"-type of operations.

Pg. 14, Para. 03.07 – Please clarify the definition for the terms "likelihood of occurrence" and "nature of the deficiency". As applicable, consider explaining any differences between the term as used here and existing audit guidance (e.g., financial statement audit guidance).

Pg. 15, Section 4 – Additional Considerations, Service Organizations – Many agencies that rely on service organizations require that these service organizations obtain SSAE16 SOC1s so that agency management may leverage these audits for A-123A (IOCFR) purposes. This model has been effective for us to reduce the overall audit impact and administrative burden. Is it GAO’s expectation that agencies continue to obtain and leverage SSAE16 SOC1s as is – or do agencies need to work with their service organizations and IPAs to modify these audits to include Operations and Compliance objectives?

Pg. 20/21, Para. 105 – The last sentence at the top of pg. 21 states that management and the oversight body should ensure that “...priorities are understood by all stakeholders, such as regulators, employees, and the general public.” How do you measure this? Is it practical to gauge the understanding of the public?

Pg. 31, Para. 4.08, “Retain” – The first bullet on pg. 31 introduces a requirement that management incentivize behavior through training and credentialing. Please be advised that there may be legal or regulatory restrictions on what costs agencies may reimburse to staff. For example, I think agencies are prohibited from paying dues or licensing fees to prof. orgs.

Pg. 31, Para. 4.11 – This para. requires that management “define succession plans for key roles, chooses succession candidates, and trains succession candidates to assume the key roles.” Please be advised that this may be a prohibited practice, at least for those agencies with collective bargaining agreements, as it creates a competitive advantage for hand-picked successors.

Pg. 38, Para. 7.05 – The last sentence of this paragraph states that “...risks could cause deficiencies in the internal control system.” Please clarify. I believe its management response or lack thereof to a risk is what may result in the deficiency, not the risk itself.

Pg. 49, 2nd para. re: “Proper Execution of Transactions and Events” – Please consider expanding on this definition. This control is more than ensuring the individuals are authorized.

Pg.’s 52-57, Principle 11, “Design Activities for the Information System” – How do these IT control related attributes relate to NIST standards? Do CIOs need to modify their IT security functions and controls if already NIST compliant?