Although I realize the deadline for comments may have passed, I wanted to take a few minutes to summarize a few thoughts relating specifically to the question "Is guidance needed to help companies determine which IT general controls should be tested?"

By way of background, I am currently an independent consultant. In my prior career, I was the Global Managing Partner of Arthur Andersen's Risk Consulting business and prior to that the Global Managing Partner of Andersen's Technology Risk Consulting business which including a significant focus on internal controls within and around application systems included what has traditionally been referred to as "general computing controls." As part of my role at Andersen, I played an major role in defining how we would work to integrate our work on "general controls" into the financial audit process. Also, although only indirectly relevant I was also involved in 2000 with the joint effort undertaken by the AICPA, the Institute of Internal Auditors, the Information Security and Control Association, the National Association of Corporate Directors and the Critical Infrastructure Assurance office to provide and education and awareness program of security issues to corporate America. The above said, I am currently not practicing as security professional but remain interested in the topic, particularly as it relates to adding value to the operations of a business and its ability to manage risk. I also believe that "security" is one area where the work that has been done at most companies as "SOX relevant" has been frequently misguided.

Lastly, I am writing this letter solely from my perspective – I am not working for any organization on this issue.

Over the past two years, I have worked with numerous Fortune 500 filers specifically relating to their efforts to define, evaluate and test "general computing controls" as part of the 404 requirements. There has been consistency in all of this work:

- Companies have identified and are testing controls that have nothing to do with potential errors in financial statements
- Because they are covering too many areas, they frequently "under focus" in the critical few areas that are relevant to financial reporting
- Companies are therefore spending money correcting "deficiencies" that also have nothing to do with financial reporting and therefore spending "millions of dollars" on issues they see as "compliance" related yet are not required
- Companies consider IT "general controls" in a vacuum without regard to other controls the organization has in place or without considering the relevance of these controls to errors or irregularities in the financial statements

There are many more common issues but these are the result. I have created a list of common issues and examples of areas that organizations are spending time on that have nothing to do with SOX and would welcome the opportunity to discuss these at any time. Although each organization has been different, when applying the "risk based" approach outlined in COSO (as well as SEC guidance) it has been my experience that most organization's have

I want to go on record as saying that <u>I do not believe that any of the issues that the companies I have worked with face are caused by either the SEC standards or guidance or PCAOB rule making.</u> Although I might have issues with the form, format and structure of the guidance or rules, the fact remains that COSO, the SEC Guidance and PCAOB AS#2 all have fairly consistently pointed out that companies were to have used a "risk-based" approach to define what risks to the accuracy and reliability of financial reporting exist in their enterprises and then define the controls that would mitigate these risks. The core problem has been that many organization's have gotten poor and self-serving advice from both consultants and auditors in this process. But a major element here is the complete lack of understanding about what "general controls" are or how they should relate to an audit of financial reporting.

So with this as a background, I offer the following comments on the specific question noted in the first paragraph. I believe that the SEC and PCAOB should totally abandon the concept of "general controls" and "application controls" and move to develop a more integrated model for controls that exist that would comprehensively define the elements of risk and control that need to be considered for the key "transaction flows" that are material to financial reporting. The end result of this process would be clarity of what needs to be tested and why – it should not be up to the SEC to define this. For purely example purposes, this model might be designed to more specifically define consider controls that are unique to each of the following areas that COLLECTIVELY achieve the objectives of internal control:

- Accounting controls – those controls that relate to classification and presentation of transactions in accordance with GAAP
- Authorization controls – those controls that relate to defining and controlling who in an organization is allowed to enter transactions in accordance with management's criteria
- Processing controls – those controls that relate to completeness and accuracy of transactions and processing of those transactions
- Program integrity controls – those controls that ensure the consistency and appropriateness of application processing logic
- Data integrity controls – those controls that relate to the integrity and consistency of stored transaction data

This is just a quick example as there are numerous issues here. The point is that the terms "application controls" and "general computing controls" are way too vague and outdated to fit in to the modern world. For example, the term "general controls" stems from the IBM mainframe environment of the 70's and 80' where all major IT activities (or at least those that were related to financial reporting) were performed on a centralized mainframe environment. In this environment, certain activities within IT were "common" to all of the applications that ran on the mainframe. In addition, most applications at this time were "custom programmed" by the IT department. Out of this environment, the concept of "general controls" was born. General controls were those that were "common" to all applications. It should be pretty obvious to anyone that this situation is no longer true. Today's large organization's have many processing environments that include a combination of purchased and programmed application systems. Each combination of application and processing environment creates a unique risk structure based on what the application does, how and where it does and who supports it within IT. The top-down, risk-based approach that the SEC wants (and which would add value to the organizations) requires that a specific and unique framework for controls exist so that management can understand specifically what it needs from a control perspective (based on the unique risks) and so that testing and any related exceptions can be properly evaluated AS A WHOLISTIC SYSTEM which is the way things should be done.

This is a complex area that require thought. The above is merely designed to provide context to what I believe the broader issue is. I would be happy to discuss these ideas at any time.

Respectfully,

Russ Gates

J. Russell Gates
Dupage Consulting LLC
2533 River Woods Dr.
Naperville, IL 60565
630-240-7580

www.dupageconsulting.com

Helping develop and sustain the maximum potential
of organizations and the people who drive their success