Cees Klumper RA MBA CIA
Amsterdam, The Netherlands

Matthew Shepherd, CPA
Boston, MA USA

January 23, 2007

Nancy M. Morris, Secretary, Securities and Exchange Commission
100 F Street, NE,
Washington, DC 20549-1090

re: File Number S7-24-06

Dear Secretary:

We herewith submit for the Commission's consideration our comments on the proposed interpretive guidance for management regarding its evaluation of internal control over financial reporting pursuant to the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 ("SOx 404").

The Commision's proposed guidance is in our view well thought-out and practical. It comes very close to supporting the efficiency improvements of 50% or greater that are achievable through the application of what we consider to be best practices in the implementation by companies of SOx 404, while at the same time increasing the effectiveness of management's SOx 404 compliance process.

The proposed interpretive guidance discusses methods that management can use to obtain evidence of the operating effectiveness of ICFR and categorizes them into on-going monitoring, including self-assessment, and direct testing. The reference in the definition of "self-assessment" provided in footnote no. 64 to "…tests of controls performed by persons who are members of management, but are not the same personnel who are responsible for performing the control" broadens the scope of activities that are now considered self-assessment. We believe that this could result in the unintended consequence of reduced reliance in the work completed by management for the auditor's assessment, as this body of evidence is now defined as on-going monitoring and not considered direct control testing.

Control testing performed by functional management (the manager directly responsible for the process) that is designed and executed in such a manner as to provide strong evidence of control operation would be akin to that derived from what in the guidance is referred to as 'direct testing' of controls. To avoid the risk of external auditors deeming reduced value derived from control testing by management, it would be beneficial if the guidance would include testing performed by all levels of management not directly executing the control with established criteria for competence, objectivity and independent verification and quality assurance, as direct testing. Testing of a control's effective operation that has been established as part of the day-to-day business routine in a functional area that is coupled with a periodic quality assessment by a highly competent and independent function (for example, by a company's Internal Audit department) can result in a quality of evidence akin to that produced in management testing completed by that independent function directly.

In our view, functional management can also effectively test controls in high-risk areas. Under its current wording, this view could be perceived to be at odds with the proposed guidance

and could conflict with the views of external auditors, which would be undesirable since it might indirectly lead to a sub-optimal testing approach.

In the attached appendices, we have described the amendments to the proposed guidance that we believe would be helpful. We highly recommend reading them for further clarification.

Appendix A is an article on the embedded testing approach that was co-authored by Klumper (one of the authors of this comment letter) that is scheduled to be published by 'Compliance Week' on January 30, 2007. The concepts underlying the embedded testing approach have been discussed by us over the past year with numerous partners and staff of the large accounting firms, as well as with officials from many companies required to be SOx compliant, both in the United States and in Europe. Klumper has during that period presented the embedded testing approach at six different public and private seminars on Internal Control, Internal Audit and/or Corporate Governance, both in the United States and in Europe. In virtually each of these contacts, the embedded testing approach was considered to be better than the current approach employed by most companies (which we refer to as the 'add-on' test approach), both in terms of efficiency as well as effectiveness.

In Appendix B, we compare the elements of the embedded testing approach to the SEC's proposed guidance, and include more detailed comments about the adjustments to the guidance that we believe would be beneficial.

We appreciate the opportunity to provide our comments. We would also very much like to discuss our comments with the SEC in a face-to-face meeting, and will contact the person(s) identified for this purpose in the Release.

Sincerely,

Cees Klumper RA MBA CIA & Matthew Shepherd, CPA

Appendix A: Article scheduled for publication in 'Compliance Week' on January 30, 2007

Appendix B: Suggested modifications to the SEC's proposed guidance

The following text is scheduled to be published as a Guest Column article in Compliance Week on January 30, 2007

Embedded Testing: A Cure For SOX Blues

By Cees Klumper
and Stephan Geuzebroek

Contrary to what you might think in the depths of an internal controls audit, it is possible to develop an approach to assess the effectiveness of controls that is both highly effective as well as efficient. The approach we developed at Ahold, which we call 'embedded testing', is founded in the most fundamental of internal control principles. External auditors should be able to place a high degree of reliance on embedded testing. Implementation of embedded testing can by itself reduce SOX 404 compliance costs by as much as 50 percent, while at the same time increasing the amount of competent evidence.

The concept of embedded testing is straightforward: testing of the operating effectiveness of a control is performed as an ongoing, natural part of the process that the control belongs to. As such, oftentimes it is executed by the manager or supervisor of the person performing the control. Test performance is adequately documented and exceptions are followed up appropriately. Internal audit departments still conduct some testing, but only to verify that managers are executing their assigned tests properly, and not to provide the principal evidence that controls are operating effectively.

With all its simplicity and effectiveness, embedded testing is nevertheless a fundamentally different approach to what almost all Sox-compliant companies do today—an approach we call "add-on testing." In add-on testing, persons who are *not* part of the regular process perform the testing. For example, these persons could be internal auditors, other internal control specialists, or persons from other departments ('peer review testing').

Embedded testing has several characteristics that make it more appealing than add-on testing or peer-review testing. Among them:

- embedded testing is far more natural;
- the cost of complying with SOX 404 is reduced by as much as 50 percent;
- significantly more evidence typically is recorded;
- control weaknesses are identified by the persons best positioned to do so;
- control weaknesses will usually be identified more quickly;
- only value-added testing activities are carried out;
- managers' control awareness is enhanced.

The Folly Of Add-On Testing

When, say, an accounting clerk performs a reconciliation of a general ledger account, typically this reconciliation is subjected to review by the clerk's supervisor in the ordinary course of business. Such a review typically wants to ensure that: the reconciliation was performed and documented in accordance with established guidelines; reconciled items could be adequately explained; possible exceptions were adequately followed up.

When the supervisor performs the review, in essence he is not adding any new information; he is simply checking—in effect, "testing"—whether the person performing the reconciliation did his job properly, ensuring that the control (that is, the reconciliation) operated effectively. In contrast, with add-on testing, someone else (for example, an internal auditor) tests the reconciliation. Essentially, that person reconfirms the supervisor's work.

Currently, many controls designated as 'key' for SOX 404 purposes are of a review, monitoring nature. As such, they would be labeled more appropriately as "tests". Managers routinely test controls because they want to be sure that the persons reporting to them are doing their jobs, that the information coming out of the process they oversee is reliable, that mistakes are caught before they cause problems, and that process improvements can be implemented to avoid future mistakes.

All this is natural; it was done long before Sarbanes-Oxley, and always will be done. It is part of the normal "Plan-Do-Check-Act" management cycle. The "check" in this management cycle is the test and it should be given appropriate credit in the SOX 404 process.

When looking at the control framework this way, having the key control tested again by an outsider (through add-on testing) is unnecessary. In fact, there is no need to do *any* add-on testing—so long as management does in fact test the key controls, in accordance with the requirements for proper management testing.

So Why The Add-On Craze?

Almost all companies have management testing performed by persons other than management: add-on testing. And since estimates are that on average, more than half of companies' SOX 404 compliance costs are spent in executing add-on management testing, it quickly becomes a very costly exercise.

So why, if embedded testing does the trick, do companies still devote so much time and resources to add-on testing?

To answer this question, recall when SOX 404 was implemented. In issuing guidance, the regulators chose to focus on the *external* auditors, who were tasked with

executing their own assessments. One trait specific to external auditors is that they are very … external. They will have no way of knowing themselves, firsthand, from their own observation, whether controls are operating as described. They must come in and test. This is the clear and fundamental difference between auditors and management: management *is* in a position (indeed, the *best* position) to know about the effective operation of controls because they are there, watching controls operate all day long, every day. They are *paid* to make sure controls operate effectively, and to take corrective action in case controls fail.

It is not as if, prior to Sarbanes-Oxley, managers were clueless, only hoping that controls were in fact working. Yet, by executing add-on testing, we are assuming exactly that: that without someone from the outside coming in, management would never know whether controls are operating as intended. Clearly this is not the case. Management has more than a clue—so why not take credit for all of the monitoring-type testing that management is already doing?

Other reasons exist why companies all went to add-on testing, some of them good. For one, without having documented all of the key controls, and having gone through to check whether they actually operated, companies were generally not too sure about where their control weaknesses were, and which managers were doing a good job of verifying this. Everything was *implicit* rather than *explicit*. Now that all key controls, including those that also qualify as management tests, as well as their operation, have been properly documented, this process has finally become *explicit*. One of the key requirements for management testing is that it must be documented adequately, since it has to be re-performable by third parties such as the external auditor. Prior to SOX 404, this was hardly ever the case. So to be able to start taking credit for the testing that management already does in the ordinary course of business, first we had to have the proof that this was actually happening. By the initial implementation of SOX, we now have that proof, managers have grown accustomed to documenting when they perform their controls (including controls that also qualify as tests), and we can start taking credit for those tests.

Another, not so good reason for why companies have generally adopted add-on testing is simply because the external auditor, unaware of a different approach, advised or even required it. From the external auditor's perspective, it makes perfect sense. To the company, however, it is a costly and inefficient way of getting the required assurance.

Finally, the add-on method is deceptively simple; typically, the approach to implementation was "first we document, then we test". So, first, all of the controls (whether they were 'just' controls or whether they were tests) were documented. Then testing plans would be drawn up for each control, and off we went—thus missing the point that many of the controls that we documented were already the tests! One positive outcome of this: where managers were inadequately documenting the performance of their tests, this was identified and remediated (in a process often called "evidence gap remediation").

Being Objective And Competent

Yes, a manager can be both objective and competent; this is the fundamental principle of segregation of duties. What would be the point of having a supervisory review, if the person performing it is not seen to be independent from the control executor? In fact, if a manager is not objective of the persons that he or she hires and fires, and cannot be counted upon to judge his subordinates' performance objectively, he should not be a manager in that position. The same goes for competence: The direct line manager should be the person most competent to judge the work of his subordinates (or certainly at least as good as any outsider coming in currently to perform 'add-on' testing). Still, to be sure, the quality of the testing performed by management should be assured through sample tests performed by internal auditors as noted before.
So while external auditors will always have to perform a measure of add-on testing, companies should not. There are two notable exceptions:

1. Where management testing would be more efficiently carried out by specialist testers. An example of this would be the store-level audit function that operates within larger retail companies. At those retailers, regional managers could be tasked with checking up on the (key) control operators, but it's just not efficient;

2. Where the knowledge required to evaluate control execution properly is so highly specialized that the company has decided it is more efficient to not have that expertise in-house , and to leave the checking up to an external party. Examples of this are the insurance company's in-house actuary, whose work is double-checked from time to time by an outside agency, or the treasury department, where a specialist could be engaging in exotic strategies and products. Some form of external oversight is often employed in this situation as well.

But these are the exceptions to the rule: that managers should perform their own management tests.

Preconditions To Remember

The first important condition is that the company's internal audit function should verify that management is performing and documenting all testing done properly.

The second condition is that managers will need to be supported on an ongoing basis in defining the appropriate testing activities (including the extent of testing, the documentation required, and so on) and in interpreting and responding to the test results. This support could be provided by the same persons tasked with all of the other required SOX 404 activities such as scoping and risk assessment, control documentation, evaluation of design effectiveness, and so on.

A third condition is that recording test activities should be made as easy as possible for management. In this regard, an effective software tool, which will also enable the company to monitor the progress and outcome of tests performed by management, may be indispensable. Where companies can still get by without an appropriate tool when using the 'add-on' testing approach—principally because the whole process is executed by relatively few 'experts'—getting many managers involved will undoubtedly change that.

The SEC, The PCAOB, And Embedded Testing

With respect to test approaches, a fundamental point that the Securities and Exchange Commission has included in its proposed new guidance for management in its execution of a SOX 404 compliant process is the recognition of the relevance and value of embedded test activities. As such, the SEC's proposed guidance provides the first (and strong) official support for embedded testing.

Meanwhile, new guidance from the Public Company Accounting Oversight Board contains one provision that in some ways appears to contradict what the SEC is proposing: namely, that the external auditor cannot make use of tests performed by managers with supervisory responsibility over the area that the control tested is part of. In our opinion, this is an unnecessary provision that could have the (possibly unintended) effect of hampering the efficiency of companies' SOX 404 compliance processes.

Shifting The Paradigm

Now that the (relatively simple) concept of embedded testing is out there, how does a company go about achieving it? Moving to embedded testing is indeed not easy. It does require the entire control framework to be re-evaluated and viewed in a different perspective. The distinction between 'mere controls' and 'control/tests' has to be defined. Controls that are not currently being tested in the ordinary course of business have to be evaluated: why is a manager not checking that this control is being performed adequately already? New controls will have to be implemented if it turns out the SOX 404 management testing was the first and only assurance we got over important controls.

And it is all worth it!

element	embedded testing approach	SEC exposure draft	comment	suggested modifications
A.	The 'embedded testing' evaluation process described herein gives consideration to all factors relevant to the effectiveness and efficiency of companies' SOx 404 compliance process.	"Management must bring its own experience and informed judgment to bear in order to design an evaluation process that meets the needs of its company and that provides reasonable assurance for its assessment. This proposed guidance is intended to allow management the flexibility to design such an evaluation process." "management, not the auditor, is responsible for determining the appropriate nature and form of internal controls for the company as well as their evaluation methods and procedures." "the proposed guidance ... allows for management and the auditor to have different testing approaches."	Although the guidance allows management and external auditors to apply different approaches, if the guidance for external auditors and for management is not well-aligned, there is a significant risk that companies will find themselves effectively being forced to adopt a sub-optimal (less effective and less efficient) assessment approach, solely in order to reduce external audit costs. This is most relevant in the area of reliance by external auditors on the work of others.	Improve alignment of SEC and PCAOB guidance affecting the auditor's use of the work of others as further described in the next point.
B.	Periodic written affirmation by the control executor, through a self-assessment program, of his or her responsibility to: 1. Execute the control as described; 2. Suggest updates to control documentation as necessary; 3. Suggest control improvements.	"These [evaluation] procedures may be integrated with the daily responsibilities of its employees or implemented specifically for purposes of the ICFR evaluation." "... activities performed to meet the monitoring objectives of the control framework will provide evidence to support the assessment."	Where the exposure draft groups self-assessment performed by a control executor together with test activities carried out by functional management, in the embedded testing approach these two are viewed as being clearly separate and distinct. In the embedded testing approach, the testing performed by functional management is designed and executed in such a manner as	Include as direct testing, testing performed by functional management (provided certain criteria for competence, objectivity and independent verification and quality assurance, are met), also for controls in high-risk areas

[1] source: SEC exposure draft footnote no. 64 "Self-assessment is a broad term that refers to different types of procedures performed by various parties. It includes an assessment made by the same personnel who are responsible for performing the control. However, self-assessment may also be used to refer to assessments and tests of controls performed by persons who are members of management but are not the same personnel who are responsible for performing the control. In this manner, an assessment may be carried out with varying degrees of objectivity. The sufficiency of the evidence derived from self-assessment depends on how it is implemented and the objectivity of those performing the assessment. COSO's 1992 framework defines self-assessments as "evaluations where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities."

element	embedded testing approach	SEC exposure draft	comment	suggested modifications
C.	Execution of independent and objective testing by the control executor's functional manager in accordance with established test procedures (see also E.)	"The evidence management evaluates may come from a combination of on-going monitoring and direct testing of controls. On-going monitoring includes activities that provide information about the operation of controls and may be obtained, for example, through self-assessment[1] procedures and the analysis of performance measures designed to track the operation of controls. Direct tests of controls are tests performed periodically to provide evidence as of a point in time and may provide information about the reliability of on-going monitoring activities."	to, in general, provide strong evidence of control operation, akin to that derived from what in the guidance is referred to as 'direct testing'[2] of controls. To avoid the risk of external auditors deeming the value derived from management testing by managers to be more limited than appropriate, it would be very beneficial if the guidance would include as direct testing, testing performed by functional management (provided certain criteria for competence, objectivity and independent verification and quality assurance, are met). In addition, in our view, also controls in high-risk areas can be effectively tested by functional management. Under its current wording, this view could be perceived to be at odds with the proposed guidance and could clash with the views of external auditors, which would be highly undesirable since it could lead to a testing approach that is sub-optimal (less effective and less efficient).	
D.	Making use of other available sources of evidence of control operation.	"Evidence that is relevant to the assessment may come from activities that are performed for other reasons (e.g., day-to-day activities to manage the operations of the business)."	The proposed guidance is in line with the embedded testing approach.	n/a
E.	Internal control experts[3], reporting to the highest levels of management, assist functional management with: 1. designing, implementing and maintaining fit-for-	The proposed guidance is silent about how companies should organize the support for the organization and execution of their SOx 404 compliance process.	It would be beneficial if the guidance were augmented. In our view, the in-depth involvement of a separate function within the organization, reporting to the highest levels of management, consisting of highly skilled	Augmenting the guidance about how companies should organize the support for the organization and

[2] The term 'direct testing' is introduced in the proposed guidance, however described only very succinctly. It is likely referring to the current 'add-on' testing approach of most SOx compliant companies. We would consider it to be a missed opportunity if it would not also encompass the concept of independent testing by line management.

[3] In many companies, an Internal Control or a similar function has been created which, among other things, has the responsibility for supporting, and executing portions of, the SOx 404 compliance process.

element	embedded testing approach	SEC exposure draft	comment	suggested modifications
	purpose internal controls, including the appropriate documentation thereof; 2. designing, implementing and maintaining fit-for-purpose tests of internal controls designated as 'key' for purposes of complying with the requirements of SOx 404, based on a top-down, risk based[4] evaluation and selection of the required controls to be tested (key controls); 3. evaluating the outcome of the self-assessment and independent (direct) testing and other sources of evidence of control operation by internal control experts in conjunction with management and control executors as appropriate.		internal control professionals, in the manner described, adds significant value to achieving an effective and efficient management assessment process in general, and robustness to the embedded testing process specifically. An Internal Control or similar function can monitor the timely and thorough execution of the tests of controls on an ongoing basis, possibly through the use of an automated tool that provides insight into such execution and the recorded results thereof. They can also 'own' the process of evaluating and concluding on, and responding to, all test results as well as to the findings from Internal Audit's assessment process (see under F.).	execution of their SOx 404 compliance process.
F.	Internal Audit independently verifies the execution of each of the above elements to gain assurance about the robustness and quality of the process executed by, and on behalf of, management.	According to the proposed guidance, this activity would be considered 'direct testing': tests performed periodically to provide evidence as of a point in time that may provide information about the reliability of on-going monitoring activities.	In our approach, Internal Audit's verifications would not be designed to provide the primary evidence of control operation (although that would be a side-benefit) but, rather, is executed primarily to "provide information about the reliability of on-going monitoring activities". Nevertheless, Internal Audit's verification activities could be stratified to also include some testing of the highest-risk controls, if that would lead to appreciably less work	See comment under B.

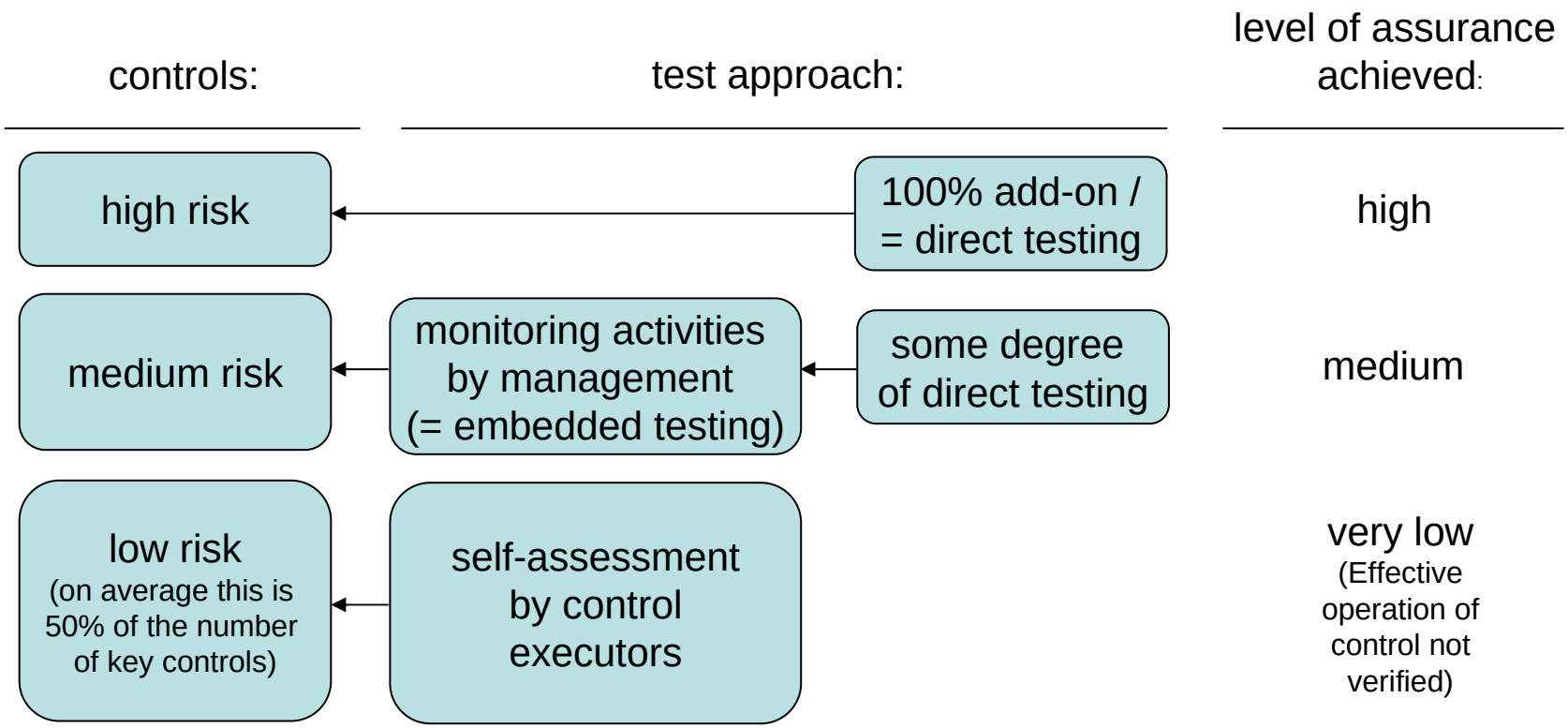
[4] this would take into account all of the relevant factors concerning inherent and residual risks; results of assessments executed in previous years; results of evaluation of company-level controls; results of other relevant monitoring activities; multi-location considerations and others.

element	embedded testing approach	SEC exposure draft	comment	suggested modifications
			having to be performed by the external auditor[5]. Again, it would be good if the guidance would specifically mention that testing performed by management could qualify as 'direct testing', provided that there is an additional check performed of the reliability of such testing as provided for in the embedded testing approach through the involvement of an Internal Control function and/or Internal Audit. A robust quality assurance process, which is executed by an independent function, significantly improves the persuasiveness of the evidence gathered through control testing completed by management.	
G.	External Audit conducts their own assessment, making optimal use of the three levels of independent assessment executed on behalf of management, in addition to the self-assessments performed by the control executors: 1. independent testing by line managers; 2. evaluation of the test execution and results by internal control experts reporting to the highest levels of financial management; 3. independent verification and quality assurance of (1) and (2) by Internal Audit.	While the SEC's proposed guidance is intended for management, clearly it would be counterproductive if anything therein would be contradictory to what the PCAOB is requiring from companies' external auditors. Unfortunately, such a contradiction at least appears to be present in the current proposal from the PCAOB (see comment box to the right).	The PCAOB's proposed guidance contains a provision that appears to contradict one of the principal concepts contained in the SEC's proposed guidance, namely the reliance by management on testing performed in the ordinary course of business. Specifically, in paragraph 15 of the Proposed Auditing Standard *'Considering and Using the Work of Others in an Audit'* states that, in order to be objective, individuals who have supervisory responsibility over an area cannot be independent in terms of testing the performance of controls in that area. As will be clear from our other comments, we fundamentally disagree with this notion. We consider it to be in direct contradiction to what the SEC is suggesting companies do. In order to achieve better alignment, the SEC	[For the PCAOB: allowing the auditor to make use of control testing performed by individuals who have supervisory responsibility over the area that they test.]

[5] Ironically, in the practice to date, internal audit testing efforts have often been directed at the **lower**-risk areas because, typically, external auditors at least place some reliance on that work where they typically have been unwilling to do so in higher-risk areas. This has then prompted companies to have their Internal Audit functions test the lower-risk areas.

element	embedded testing approach	SEC exposure draft	comment	suggested modifications
	The embedded testing approach was developed with feedback from external auditors to emphasize a reduction in the total compliance cost to companies.		and the PCAOB should consider recommending companies employ an evaluation process to determine the level of independence and objectivity. This evaluation should include the following criteria: • Extent of supervision, guidance and review provided by independent "SOx experts", including development of test procedures, review of workpapers, training, quality assurance, etc. as described herein under E. • Existence of policies governing SOx compliance, • Competence of tester in the subject matter • Policies linking timely and accurate control testing to the employee's job functions, • Existence of a control environment that supports and fosters timely and accurate SOx compliance activities. We will also direct this point separately to the PCAOB.	

likely average interpretation of the proposed guidance:

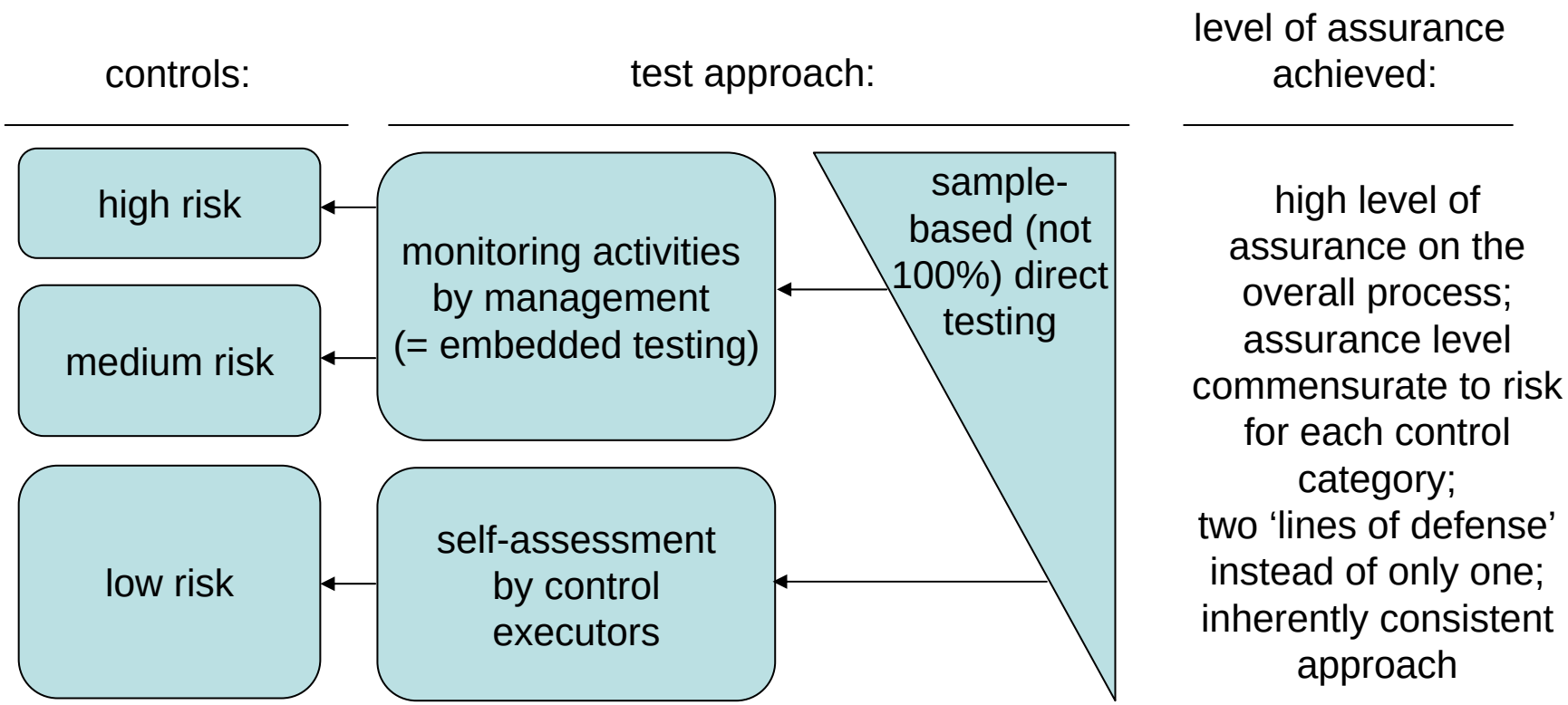


required SOx-specific effort level (pre-new guidance level = 100%): 70%

total assurance achieved: moderate; quality assured for only medium and high-risk controls

"frustration level": remains fairly high due to continued inefficiencies because of 100% add-on testing requirement for high-risk controls and fundamentally inconsistent testing approach for the different control categories

a better alternative, with only minor tweaks to the proposed guidance:



required SOx-specific effort level (pre-new guidance level = 100%): 35%

total assurance achieved: high level of assurance that is commensurate to risk

"frustration level": lowest possible; natural allocation of responsibilities between management & internal audit; no unnecessary duplication of effort; only value-added test activities by the right people