	Question	Grouping	Original List #
Questions selected for a specific response:			
1	What supporting evidence (besides a charter or code of ethics) is used to test the effectiveness of the board and audit committee alike? **Answer: The evaluation of the effectiveness of the board and audit committee starts with a self assessment process, which formally provides the opportunity to determine how they are meeting their responsibilities. Further, records of meetings, actions taken, discussion and direction provided, oversight approvals, and frequency of meetings are evidence of their effectiveness.**	Audit Committee	1
2	The guidance and also the audit standard No. 2 do not address disclosure control issues that are not linked to accounts. **Answer: Principle 15 speaks to financial reporting and addresses the need for good communication within and outside of the organization to ensure information is appropriate and controls are working. Under this principle, the organization needs to have in place controls to ensure that information is collected, distributed, analyzed, and reported appropriately to those who need to know. The oversight of what constitutes the appropriate information for disclosure is, in part, regulated. However, from the standpoint of good internal control, sensitivity to information needs should be evident by the organization's actions to ensure disclosures are complete, accurate, timely, and written in a language that can be understood by the reader.**	Control	6
3	How does the existence of insurance coverage for loss affect the evaluation of control activities? **Answer: The use of insurance is a control technique whereby the organization has agreed to "share" the risk of a particular exposure with an outside party (the insurance company). The assessment of this control would focus on the "unmitigated" risk beyond what has been shared with the insurance company, and how the organization manages that risk. This is true when insurance cannot be obtained to cover the entire exposure or when management only wishes to cover extreme situations and thus is willing to accept a large deductible or assume excess exposure. However, it is important to note that the guidance is for internal control over financial reporting, with an objective to ensure reliable financial reporting for external reporting purposes as well as management decision-making. The risk of misstatement or control failure is not something that a company can usually insure against. Therefore, the question regarding insurance coverage is more applicable to the other control objectives in COSO's *Internal Control -- Integrated Framework*, i.e. compliance and operations.**	Control	9
4	Does the guidance state or explain to managers that the need for risk assessment and appropriate internal controls is an ongoing process, as opposed to an isolated event?	Control	11

	Answer: The guidance clearly states that internal control is a dynamic part of the organization and not a once-a-year event. The guidance emphasizes the need for a strong risk assessment process that is ongoing and monitored for its effectiveness. Continually reevaluating the environment in which the organization exists is necessary to ensure the proper controls are in place to meet the changing needs of the organization as it grows. The COSO Framework reiterates that control evaluation is a continuous process. The guidance encourages management to take full advantage of all elements of the model, including updating risk assessment as necessary, and perhaps as importantly, implementing effective monitoring to assure management that other controls are operating effectively.		
5	David Richards mentioned that entity-level controls should be at an appropriate level of precision. He gave an example that budget-to-actual comparisons on a quarterly basis wouldn't be an adequate level of precision. Due to familiarity with the numbers, in many small companies the CFO can look at a comparison and identify problems at a glance. What would be an example of a control or combination of controls that would have adequate precision in this situation? **Answer: The question addresses a difficult issue. i.e., whether management review is a monitoring control or a control activity. Generally, controls should be built into processes, not added on. The review of an organization's performance is a compensating control designed to catch the failure of specific controls that were put in place to prevent or detect an undesirable situation. Review by the CFO is a key backup control but should, in most cases, not be relied upon to replace front-line controls designed to prevent or detect information, transaction, or processing errors. Regarding the situation posed in the question above, an example is for management to review weekly sales data and compare it with orders, or to compare it with sales data for a comparable period, or with sales data seasonally adjusted for trends in sales. A second example is for management with knowledge of the level of activity to review weekly payroll and the number of employees to determine that the weekly payroll is correct. This is a management control and provides indirect evidence on the working of controls.**	Control	13
6	How will this new guidance increase reliance for management and external auditors on entity-level controls (versus the more common emphasis on 404 testing focus on discrete process controls)? Is the risk assessment guidance provided here agreed to make this shift?	Control	14

	Answer: Generally, the term "entity-wide controls" refers to the control environment component of the COSO internal control model. In some cases, we also have found that individuals use the term to refer to controls that are implemented throughout the organization, e.g. standardized computer control processes. In answering the question, COSO reiterates that all components of the internal control framework are important. However, the task force certainly felt the control environment, to which almost one-third of the principles relate, is important. In some sense, the control environment can act as the first, but not the only, line of defense against the risks that affect the reliability of the company's financial reporting. The guidance reiterates the centrality of risk and its relationship to controls. In other words, controls exist to address risks – essentially to mitigate those risks and to bring them down to an acceptable level. There is guidance on performing the risk analysis and linking it to the internal control evaluation process.		
7	Risk is measured based on impact and probability. Do internal controls affect only the probability or both the impact and the probability? **Answer: Internal controls are put in place based on the materiality (impact) of a risk on the organization and the perceived likelihood (probability) that the risk would be realized if nothing was done. Thus, the determination of when a control is necessary should be based on a risk assessment with a linkage to control activities that are put into place to address the risks. Further, the guidance encourages management to evaluate the cost-effectiveness of alternative controls designed to address the risk.**	Control	15
8	If an organization happens to have more than one control that addresses the same attribute and wants to control costs, would it be acceptable to test and rely on only one of the controls, even if the other controls continue to exist? **Answer: If an organization uses multiple controls to address a particular risk, then the organization should be clear as to the intended result of the controls. Generally, the answer to the question should be yes; i.e., if one control completely mitigates the risk, then that control is the one that should be tested. However, the organization should consider why it has implemented potentially redundant controls with the same objective. Often a redundant control may address another risk that is mitigated only by that control. Thus, to be cost-effective, redundant controls should have a purpose and the assessment process should provide clarification that the redundancy is actually needed.**	Control	18
9	Many small companies are fast growing with continuously evolving operations, processes, and controls. How does the committee recommend that a small company cost-effectively remain in compliance with the Framework when facing a moving target?	Cost	19

	Answer: The importance of a vibrant risk assessment process is the key to the changing environment of the organization, for financial, operational, and compliance controls. The guidance suggests that process owners be charged with an ongoing assessment of new risks and with the implementation of controls to address those risks. The transaction processing system needs to keep pace with the growing business, so that incorrect processing risks are effectively mitigated. This is important, not only for 404 reporting, but also for helping ensure the success of the organization. As the company grows and evolves, the guidance suggests that oversight (such as a risk management function, internal audit activity, or the corporate controller) be utilized to update the risk assessment and needed controls.		
10	Can you comment on increased audit costs and expand your comments on costs incurred by other small companies for 404 compliance? **Answer: Costs incurred to assess internal controls will vary depending on the complexity of the organization, geographic dispersion, business processes, technology utilization, and other factors. Regardless of SOX 404, COSO believes that a good internal control system is necessary and thus relating the cost of internal control to SOX 404 is not the right perspective. If controls have been properly built into systems and a good monitoring process exists, compliance with SOX 404 is inherent and little "extra" work would be needed. COSO is not in the position to comment directly on audit costs. However, we believe the guidance will be useful to both management and external auditors in potentially streamlining their assessment of internal control. This guidance, coupled with forthcoming guidance from the PCAOB and the SEC will assist all parties in controlling audit and compliance costs.**	Cost	22
11	Does this guidance enable a cost-effective audit of internal controls for smaller companies? **Answer: "Cost -effective" is a relative term. The guidance discusses the framework for a good internal control system. It puts into print real examples of how small businesses have already put in place (without SOX 404) internal controls to address the 20 principles. Cost-effective internal control is an ongoing effort by which controls are continually evaluated as to need, effectiveness, and changing environment. If an organization follows a good risk assessment process to determine vulnerability to key risks, and reacts by putting in place techniques to mitigate those risks, then the process should be cost-effective.**	Cost	24
12	What average costs have other small businesses encountered in implementing and sustaining the COSO regulations? **Answer: We are not aware of any study that provides this type of information. It is difficult to determine what organizations have already invested in internal control techniques versus the assessment costs that seem to be the focus of most organizations today. COSO believes that the monitoring principles display how a good organization should build an ongoing assessment of internal control. This makes the SOX 404 work much less onerous on organizations.**	Cost	29

13	Does COSO provide any guidance on assessing the severity and implications of control deficiencies? **Answer: The Monitoring Principle # 20 speaks to the reporting of deficiencies. COSO has not tried to define deficiencies in the same context as the PCAOB has done for external reporting purposes. COSO believes that the board and management need to be made aware of ineffective internal controls and plans for correcting the situation. In most organizations, this level of oversight incorporates, but goes far beyond, defining reportable deficiencies so that the oversight functions can appropriately address situations that (if left unchecked) could lead to more serious issues.**	Deficiencies	30
14	Small companies often have few finance/accounting personnel. How does the newly issued guidance for smaller public companies address the potential for "segregation of duties" control deficiencies arising at smaller companies? **Answer: In the guidance, one of the challenges of a small business is recognized as appropriately implementing a "segregation of duties" structure. However, the guidance recognizes that other types of controls could be used in lieu of segregation of duties; e.g., periodic summaries of transactions, reviewed by a person other than the employee recording the transactions. These summary reports look for unusual or high–dollar transactions. The guidance also points out how effective information technology (IT) controls might be used to address potential segregation-of-duties risks. The key point that the guidance makes is that each organization needs to assess its risks and to implement controls that mitigate the risks to an acceptable level. As the company grows, the addition of personnel may allow for better segregation of duties. While it is growing, the organization should consider a combination of controls to mitigate the risks that are exacerbated by ineffective segregation of duties.**	Deficiencies	35
15	Many smaller companies set the right tone and monitor well, but lack documentation of these controls, particularly the monitoring controls. Will/can a company get "credit" for controls that are undocumented and if so, will the PCAOB agree? How should the client and its external auditor document what is undocumented?	Documentation	37

	Answer: The guidance discusses the need for documentation and recognizes that in small businesses, the documentation of a control may reside in its exercise, not in its written documentation. However, when public reporting is required, there is a need to provide evidence that the control is working. Documentation in small businesses, while required, may be less extensive than that needed in larger companies. The guidance presents numerous examples of less formal, but effective, documentation techniques. As organizations grow, documentation helps communicate essential responsibilities. It is important that businesses recognize the need to be able to 'prove' that controls are working. This requires something more than management's assertion and the absence of material financial statement adjustments. Management can and should be prepared to present the case that less formal documentation is still documentation. Management and the auditor should jointly assess whether the documentation level is sufficient to meet the reporting needs.		
16	What functional area of the company should "own" documenting and assessing the 20 internal control principles? **Answer: COSO clearly believes that ownership of internal control is a management function and should rest with the owner of a business process. The process owners should ensure the appropriate levels of control for their processes, enable communication / training on how the controls should work, provide ongoing monitoring of the effectiveness of the controls, and be accountable to management for the overall effectiveness of the control structure for their processes.**	Documentation	38
17	How do we document management's own detailed involvement in internal control? Can a smaller company depend on this as a critical part of its internal control system? **Answer: The guidance discusses the involvement by management as a key difference between the small and large organizations. The fact that management takes a more active role in the day-to-day operations of the business provides better understanding, reinforces what is expected and important, and ensures a more ongoing awareness of the effectiveness of controls. Management's involvement is a key control environment factor that sets the tone for good internal control. It should not, however, be relied upon as the sole means to control transactions, as it is rare that management would be involved in every transaction of the business. Management oversight (monitoring) is also a key factor in the overall control structure, and should be included in the determination of the effectiveness of the internal control system.**	Documentation	40
18	Can less formal documentation mean narratives without flowcharts in the 404 docs, for example?	Documentation	44

Answer: Documentation is discussed at length in the guidance to provide a context for determining the appropriate level and methods that can be used. Flowcharts are not the only methodology to achieve effective documentation. Narratives or other methods that effectively identify the controls, responsibilities for ensuring the controls work, and operations of the controls are acceptable. Often new system implementation documentation is the best source of an overall design of internal controls. The key here is the ongoing upkeep of this documentation, which is an issue for both small and large organizations. Thus, control documentation needs to be a responsibility of the process owner who can determine the appropriate level of documentation needed to ensure the controls exist and are understood, as well as provide a framework for assessment. Technology solutions are often required in documentation when interfacing complex computer systems and manual operations..

19	Discuss the level of documentation expected for business processes and their controls and supporting IT. Answer: The level of documentation will vary based on the complexity of the process and the diversity of use. Organizations with one location need less documentation than those with many locations and actions performed by multiple people. The degree of computerization impacts the need for documentation. Systems documentation generally is more specific and detailed in order to ensure a change control process exists. IT controls are a specific principle (#14). A high-level document is created to put into context the interface of steps within a process with control gaps. Detailed instructions may provide supporting documentation to guide individuals who are performing the control, and to ensure that specific procedures are followed, exceptions are documented, issues are dealt with, transactions are analyzed, etc.	Documentation	46
20	Documentation has been a struggle for small companies even though controls are performed. What would be adequate documentation of a review of a comparison, analysis or reconciliation? Same question for other types of controls?	Documentation	47

	Answer: The guidance provides information on what form documentation can take. Generally, documentation of comparisons, analysis, or reconciliations can be evidenced by: **• Initials indicating the review was performed.** **• Notes on the document (the comparison, analysis, or reconciliation) of exceptions noted and a reference to follow-up action to be taken.** **• The result of the follow-up work (either on initial document, or on another document).** **The evidence must be sufficient to persuade a reasonable, unbiased observer that the work was performed, and was performed in conscientious fashion. Monitoring is clearly documented in formal assessments, but in routine, ongoing monitoring, the actions taken may be evidenced by sign-offs, approvals, or actions taken as a result of the monitoring step. Thus, assessing internal controls on a routine basis should be documented to the extent necessary to historically document the organization's exercise of responsibilities. This is a management decision based on the ultimate needs of the organization.**		
21	How can the guidance help to minimize identity theft and fraud? **Answer: Principle #10 speaks to fraud risk assessment. It recognizes that fraud risk is one of many risks an organization can encounter and that it deserves separate attention by management in the overall design, implementation, and monitoring of controls. A formal risk assessment process should include a thorough evaluation of the vulnerabilities of the organization to theft and fraudulent activities. In practice, fraud risks often look like risks due to other errors. Often the threat of fraud or theft can be addressed when the organization considers the impact, and likelihood, of a risk that would result in the loss or inaccurate recording of transactions. However, specific risk assessments should also include the signs of fraud or theft that can be evident in a good and effective control environment.**	Fraud	48
22	Does the guidance focus on internal control over financial reporting or does it equally apply the guidance to operational and compliance internal controls as well? **Answer: The COSO Small Business Guidance was specifically developed to address the financial reporting objective of internal control. Thus no specific reference is made in the document regarding its applicability to the compliance and operational objectives. However, COSO generally believes that the 20 principles should provide a good starting point for determining the adequacy of the internal control systems. There may be some differences but, in general, this framework could be used in the assessing of compliance and operational control systems.**	Framework	51
23	In the 1992 COSO and in the ERM guide, risk responses are part of the risk assessment components and control activities are what management does to be sure the risk responses are working. In this guide it appears those responses are in Principle #11 and a part of control activities. Is that a change, and how much does it matter which principles match up to which categories of control?	Framework	53

	Answer: You are correct that the determination of the right risk response (share, control, accept, or eliminate) is a separate decision, by management, that stands apart from determining the appropriate control to put in place to reduce the impact on the organization of a given risk. However, Principle #11 recognizes that controls need to be implemented to mitigate the risks. When talking about the risks associated with financial reporting, management needs to identify specific controls because it is not possible to share the risk. Management must choose to control or eliminate the risk. If the risk is not significant, management may choose to accept the risk. The intent is to be consistent with the COSO 1992 Framework. As noted earlier, internal control is a process. We hope users of the guidance will understand internal control as a process, and identify appropriate controls to mitigate risks in order to achieve effective financial reporting.		
24	If a company had fully and effectively implemented the 20 COSO principles as well as the corresponding controls, would it be logical to assume that the company would be SOX compliant assuming all the controls were working appropriately? **Answer: Yes, COSO believes that when an organization properly addresses the 20 principles that would provide a solution that would more than adequately address the SOA rules. The degree of attention to internal controls in most organizations goes well beyond the "key control" concept. Thus, when management properly assesses risk and determines which risks must be mitigated, that will usually identify a much larger number of risks for mitigation than is currently the focus of SOX assessments.**	Framework	54
25	Does the guidance provide an illustrative example/template for scoping financial statement balances? **Answer: The guidance provides examples of how an organization might evaluate which accounts are more significant than others (Volume III). The determination of which accounts are significant is relative to each organization and thus no "one size fits all" template can be suggested. However, the examples in the guidance provide a breadth of factors that can be used in making this determination. The selection of accounts to be reviewed depends on the materiality of the account to the overall financial results -- not necessarily on the account's balance. Thus, the guidance discusses the need (and options) for setting a materiality threshold for determining subject matter that has a significant impact on the overall financial results.**	Framework	56
26	Why is this guidance based on the five-component framework versus the newer eight-component COSO framework?	Framework	60

	Answer: The COSO ERM guidance issued in 2004 was intended to assist in the further guidance on how to develop an effective ERM program. The additional components included in that document were intended to further explicate the risk component of enterprise risk management. The consistency between the 1992 document and the ERM guidance is not a coincidence. Both represent a systematic process for identifying and controlling risk. The 1992 document is a sufficient framework for evaluating internal control over financial reporting. Effective ERM is an important goal for companies and can be used to address financial reporting objectives as well. Having a full ERM approach is desirable but not necessary for compliance with the Small Business guidance.		
27	Operations and compliance are also internal control components, however, the guidance seems to heavily emphasize financial reporting, a-la SOX. Will there ever be guidance regarding operations and compliance? **Answer: The COSO small business guidance document was intended to address only the financial reporting objective of internal control. That said, COSO does believe that the 20 principles and related attributes provide a sound foundation for evaluating compliance and operational objectives as well. COSO believes that the compliance and operational objectives of internal control are as important as the financial reporting objectives and should not be ignored by businesses. Further, many financial controls are being incorporated into operating processes; therefore, most businesses have to consider their operating processes in evaluating internal controls over financial reporting.**	Framework	63
28	Sounds the same as regular COSO. I'm not clear as to what is different other than providing "templates" and "guidance" which also exist for regular COSO from consultants. Can you please give more examples of what you mean? **Answer: The COSO small business guidance provides specific examples, approaches, and tools – directed toward small businesses – to help them understand their options when implementing the Framework. The principles and attributes were mapped to the 1992 document, during the development of this new guidance, to ensure consistency and continuity of the documents. The small business project confirmed, to COSO's satisfaction, that the Framework produced in 1992 is still as applicable today as it was then. The display of the principles and attributes provides an easier way to view the concept of internal control, and help management and others determine the proper level of controls needed for a specific organization.**	Framework	65
29	What are the implications of suggesting a principles-based guidance in a legal environment so enamored of rules-based interpretations? Might there be added legal consulting costs that lessen the 404 compliance benefits you have described?	Framework	66

Answer: The COSO guidance is principles-based so it can be applied over time and can provide a framework for the development of internal controls. Rule-based guidance is left to the regulatory agencies and is generally intended to provide consistency of assessments against a principle-based framework, such as the COSO Framework. The COSO task force felt it was important that management have the ability to select among a number of controls and be able to choose cost-effective options for achieving financial reporting objectives. That selection requires judgment. However, the bottom line is whether the controls are effective in achieving the desired objective of reliable financial reporting. COSO believes it is better to empower management to make these decisions and that reasonable people can agree whether the choice of controls assists in achieving the objective. Reasonable judgments, justified and verified through independent assessment, should not necessarily lead to more litigation.

30	Is it appropriate for the internal audit function to assist in the documentation of controls and completion of the risk assessment, as long as they do not have a role in the implementation and/or design of the controls themselves? Answer: The internal audit function is generally viewed as part of the monitoring aspect of internal control. To be truly independent of that process, the internal audit function should be outside of the details of the control design, documentation, and ongoing monitoring that management performs. COSO understands that many organizations have turned to internal auditing to assist management in the documentation of their controls systems and to act as an adviser during new systems development. This is an acceptable role for internal auditing. However, the processes and the control assessment are clearly a management responsibility. They should assist senior management and the audit committee in ensuring the appropriateness of process-owner control design and testing.	Internal auditing	69
31	Could you clarify with respect to the question of emphasis on the evaluation of general IT controls vs. application controls? Answer: General IT controls assist the organization in the nonspecific system techniques used to ensure the integrity of computer applications (e.g. change controls, backup and recovery, documentation standards, etc.). Application controls deal with specific controls built into a computer system, specifically designed for that system, and based on the transactions and processing performed in the application. Application controls tend to be routine in nature and often occur without the knowledge of the user, unless an exception is noted. Application controls tend to be more relevant to overall financial reporting because they are designed to ensure the completeness, accuracy, and timeliness of data. Application controls also play an important part in defining what controls are built into an application – as opposed to those that may be manually performed outside the system but are nonetheless important to the overall integrity of the process.	IT	73
32	How does the new guidance for small businesses treat IT security as part of the compliance	IT	74

	process? **Answer: The information technology principle (#14) discusses various aspects of how technology controls impact processes. It does identify the need to look at overall application access security in designing internal controls – especially when structuring specific transactions that can be executed by an individual vs. others. Overall computer access is also identified as a key control to ensure information is kept secure from intrusion or unauthorized modification. Security is an area of risk where the organization has to determine what specific risks have the potential to occur within the operating environment. The security of computer systems is as much an issue as the overall physical security of information.**		
33	Does the guidance provide tools to document general IT controls, and what level of testing is suggested for application controls? **Answer: The COSO small business guidance document has a section within Volume III (Tools) devoted to IT examples for various types of computer environments. Although not prescriptive, these examples provide a starting point for organizations to assess their general and application controls relative to the ultimate purpose for the control (i.e. prevention of detection). Testing of controls will vary depending on the magnitude of the transactions handled by the application and the frequency of those transactions. Monitoring of internal computer controls should address the ongoing and special assessments performed on these key controls.**	IT	78
34	Applying entity controls and IT general controls seems to be more of a check-the-box process than other controls activities. Do you think you can effectively apply these higher-level controls and reduce other control activities or do these higher-level controls only have a downside on the amount of compliance work to be done? **Answer: The COSO document recognizes that general controls and application controls have different purposes. To rely solely on either one would cause the organization to be exposed to the risk of inaccurate information. The complexity of the organization, its geographic dispersion, the number of computer applications, and other factors will influence the degree of general controls needed. Application controls, regardless of whether they are in-house or outsourced, need to be designed and monitored for effectiveness. Control techniques can be incorporated, other than at the detailed transaction level, and still provide a high level of confidence in the data collected. These techniques would need to be sufficient to address the control objectives necessary to mitigate the risks identified. Small businesses should have a better opportunity to use higher-level controls, because of the relatively small number of transactions compared to the number done by a large business.**	IT	86
35	How do you define management? Specifically, who should be responsible for managing risks and who should be responsible for managing internal controls? If it is the same person or group, wouldn't that be a risk in itself?	Misc	91

Answer: Management is the individual within the organization who has been charged with the responsibility for oversight of specific business operations. Management is a general term that refers to the structure used by an organization to ensure things get done according to design and plans. Management usually has specific defined roles and responsibilities assigned by senior leadership of the organization or the board of directors. This formal delegation is often reflected in organizational charts, mission statements, responsibility guides, charters, or other general business guidance (such as policies or procedures).

36	We're currently setting up a new small business that resulted from the sale of our department from a large corporation. Will Volumes II and III assist us in setting up our new company? Do the volumes give examples of setting up controls for wiring money, cutting checks, processing accounting transactions, etc.? Answer: The COSO guidance document provides an overall approach. The overall Framework provides an approach to addressing the control environment subject areas to be addressed: the approach to risk assessment, the selection of the right controls to address the mitigation of risk desired by management, the identification of what information needs to be communicated to whom, and the inclusion of monitoring techniques to address ongoing and special-purpose reviews. Fortunately, there are many places you can look to find specific controls for areas such as wiring funds. COSO identifies the specific control considerations that address the risks associated with wiring funds. Those risks might include: unauthorized wiring of funds, incomplete transmission of the message, incorrect amount being wired, incorrect recipient, incorrect time period, interception of the message and the ability of the interceptor to then hack into the company's records. Many internal control publications provide specific examples of how an organization can mitigate those risks.	Misc	95
37	What kinds of resistance will likely occur when we try to develop effective internal controls in small companies? And how do we cope with these problems? Answer: Normally, the resistance to implementing an internal control assessment process is the perceived burden of time and money to be expended to complete the process. Results to date have shown that those organizations that have paid attention to their internal controls will most likely discover things they did not know were happening in the organization. These include controls not working as intended, controls that are not in place, controls not needed, controls results not being addressed, and a general lack of awareness of the need for, and expected results from, using controls. The fact remains that well-managed organizations require good internal controls regardless of regulation. Regulation should not be a reason for implementing controls. Good business practices should drive the selection and overall results of good internal controls. It only takes one Enron to see the impact of poor controls on a business. Thus, the emphasis often is on the cost to implement versus the cost to the business if controls fail.	Misc	96
38	Please clarify exemptions.	Misc	100

Answer: COSO does not believe ANY organization (public, private, government, not-for-profit, etc.) should be exempted from good internal controls. Every organization has an obligation to its constituents (lending institutions, shareholders, employees, public, etc.) to have processes in place to ensure the mission of the business is being properly accomplished, the information provided is accurate, disclosures are based on openness of communication, and the integrity of management can be trusted. Thus, although the SEC is considering levels at which public disclosures by certain size organizations would not be required, COSO believes that does not mean those who do not have to make a public statement should conclude they are not responsible for having good internal controls.

39	When doing the risk assessment, is materiality still the underlying main criteria? For example, fixed assets constitute routine transactions with little risk. However, because it is material, do we still need to address it? Answer: Risk assessment is a key factor in determining what controls are needed. Materiality has its place in helping management determine risks and the associated need for controls. When assessing internal controls, management should consider ongoing needs to make sure specific controls that are deemed important to the process (that may not necessarily be material) are functioning as designed. It often is difficult to put a price tag on the results of an undesirable risk that is tough to quantify but obvious in its impact (e.g. reputation risk in the case of a company like Arthur Andersen). The question explicitly cited fixed assets as an area of low risk. However, it is important to note that it is not necessarily low risk. There is fraud risk (WorldCom), valuation risk, as well as transaction processing risk. Each organization has to assess the risks associated with its account balances and disclosures.	Misc	102
40	Panel question. I work for an offshore auto parts manufacturer. I formerly worked as a controller for a public company and am very familiar with SOX404. In response to internal control issues, I get the response, "We're a small company. We do not need control like that.." Will the COSO guidance help me in getting our company "over-the-hump" and develop a more stringent internal control system? Answer: Yes, the COSO guidance was designed to help you in addressing this very issue. Often, organizations feel that controls are applicable only if you reach a certain size. The realities of life say that controls need to be in place right from the start. They will change in quantity, frequency of application, complexity, etc., as the organization grows, but their presence is undeniably obvious and directly proportional to the success of the business. History shows us that many businesses without controls soon find themselves out of business.	Misc	105
41	What tools do you recommend to help determine the soft controls related to a company's control environment?	Misc	109

Answer: The COSO document provides in Volume III (Tools) several samples of ways to get an overview of the controls in place that reflect the control environment. For each principle and related attributes, the guidance offers ways to document the presence of control techniques being used to address the attribute and what evidence might exist to confirm the effectiveness of the control. Soft controls generally tend to be organizational in nature and are a direct result of the management's recognition of the value of a good control environment. In such an environment the focus is on ethics, assignment of authority and responsibility, dealing with human resource policies, and other indirect controls that shape the organization's overall support for driving a culture that respects the need for control.

42	Does the guidance provide example measures for calculating materiality, especially when pre-tax income is not the most relevant basis? Answer: The COSO guidance does discuss the use of materiality to help the organization to focus on areas where controls are needed. Materiality is a factor in determining what level of precision of the effectiveness of a control may be necessary. Not all controls deal with financial materiality; some deal with other important aspects of the organization's compliance and operational effectiveness. It is important that the organization come to an understanding of how it will determine what is material to its results, especially when faced with competing needs and limited resources. Material transactions are discussed in the document in light of how they impact the financial reporting objective of internal control. Materiality for the other objectives of control (compliance and operational) may take on a wholly different perspective.	Misc	112
43	What efforts are planned to get the word out “world-wide”? Will this guidance be translated? And, into what languages? Answer: The COSO document will be translated into other languages, as have prior versions. Translated documents will become available over a period of time. However, this will take some effort to coordinate. A process is in place for those wishing to translate the documents to contact COSO and establish an agreement.	Misc	115
44	Who should develop risk matrix: management or internal audit? Answer: A risk model should be developed for the organization and should contain a wide variety of risks that could be incurred by the organization, given its industry, location, and operations. The risk matrix -- the application of the model to a specific situation -- should be prepared by management. Internal audit often facilitates these discussions in order to help ensure the consistency of the assessment process across the organization. If an ERM element exists, it would generally facilitate the process by providing structure to the approach, quantification of risks, setting likelihood guidance, and determining the appropriate response to the risks identified.	Misc	116

45	I'm hearing that you'd like small businesses to be on the same page when it comes to internal controls (for the sake of the auditor?), but is that taking into account that owners/managers of small businesses have different skill levels to be able to participate in the process? **Answer: The owners of small businesses are expected to have a wide variety of skills in order to be effective in managing their businesses. It is true that the owners will need to assign someone in their organization to provide the necessary drive to complete this assessment. Often, owners will turn to their internal auditor, controller, or CFO to champion the project within the organization and to provide structure to the process.**	Misc	120
46	Does any of this guidance change the relationship a company should have with its external audit firm? **Answer: No, the guidance does not fundamentally change the relationship between the internal auditor and the external auditor. External auditors have experience in assessing internal controls as part of their financial audit work. Thus, their knowledge of the organization's internal controls should be helpful to the organization. The guidance encourages management to have ongoing discussions with the external auditor about the design and implementation of internal controls.**	Misc	124
47	Does this apply to nonprofit organizations also and in what way? **Answer: COSO believes that this guidance has application to all types of businesses regardless of size. Public, private, government, not-for-profit, etc., businesses should pay attention to their control structure and use of the 20 principles and associated attributes in this document. The principles apply to all organizations as a framework upon which to design and build internal control structures, and provide a basis from which to construct assessment methods.**	NFP	126
48	Does the guide touch on the evaluation of third party providers and the use of Type II SAS 70s in assessing internal control over financial reporting? **Answer: The guidance includes a discussion of outsourced operations and how those situations require a different approach to internal control because the organization does not directly process or influence the specific controls used by the provider. The use of outsourced operations is fairly common in small businesses. This creates a unique situation wherein identification of internal controls, within the organization, to manage the quality of the information supplied by the outsource provider is an important consideration. Management reviews and analysis take on a higher level of importance in these situations and specific documentation may be needed to ensure that reviews are being conducted with consistency.**	SAS 70	129
49	What is the relationship between this COSO project and the SEC's announced intent to provide more guidance to the smaller public companies?	SEC	131

	Answer: COSO was asked by the SEC to look into guidance provided to small businesses regarding internal control. COSO believes the small business document provides that guidance by helping small businesses understand the breadth of options available to them within the COSO Internal Control --Integrated Framework. The SEC is continuing to review the results of its Small Business Task Force and will issue guidance to organizations regarding public reporting, management's assessment process, and auditing requirements. COSO's position is that internal controls are a management responsibility regardless of the size of an organization and that regulatory reporting does not remove this responsibility		
50	As practitioners, what we would really like you to highlight, is how your guidance for a small cap company would differ from your approach to a large cap company that is subject to internal controls over financial reporting? **Answer: The COSO guidance concludes that the only difference in internal controls between large and small companies is the degree of implementation. Large organizations need more complex internal control systems than smaller businesses. The approach outlined in the COSO small business guidance can be used by small and large organizations. The 20 principles and related attributes are not unique to a particular size organization. They are applicable to all businesses.**	Sm Co Difference	139
51	How do you define a "small company"? **Answer: Although the concept of "small" has occupied a considerable amount of discussion with the SEC, COSO concluded early on that the principles and related attributes apply to businesses of all sizes, and thus little time was spent dwelling on the definition of the term "small business." Included in the COSO document are a set of characteristics and a discussion of the differences between a small and large organization. In conclusion, COSO states the difference lies in implementation of the principles not in the principles themselves. Thus small businesses still need to pay attention to how they implement the control principles. The COSO guidance provides examples, approaches, and tools specifically drawn from the experiences of small businesses that should assist in addressing this subject.**	Sm Co Difference	144
52	Is there a size of company to which this document no longer applies in terms of revenue and market capitalization? If so, what amount of revenue, and what market capitalization? **Answer: The direct answer is no. COSO believes that this guidance has application to all types of businesses regardless of size. Public, private, government, not-for-profit, etc., businesses should pay attention to their control structure and use of the 20 principles and associated attributes. The degree of implementation will vary with the size of the business but the principles should still be evident. As noted earlier, good internal control is good business and should lead to an increased survival rate among smaller businesses**	Sm Co Difference	161
53	Smaller firms may have smaller sample populations for testing of key controls. How should an auditor measure the effectiveness of a key control in the event of a small population?	Testing	171

Answer: The level of testing of transactions is designed into the test plans and should be correlated to the objective of the test (e.g., to confirm the control is in place and working versus the control is effective). Sample sizes will correlate to the expectation of precision desired in the outcome. Test plans should clearly indicate how results will be interpreted and what level of error or variation from expectations is allowable (e.g., no errors should be found).

54	How does the new framework assist in emphasizing entity-level controls and possible reductions in testing of the individual processes?	Testing	173

Answer: The COSO guidance emphasizes that entity-level controls are different from individual process controls and should not be viewed as overriding or supplanting the need for individual process controls. The need to perform overall assessment of the quality of the organization's control environment, risk management, information and communication processes, and monitoring techniques, is critical to the overall assessment of the organization's internal controls. Volume III (Tools) provides templates and examples of how such an assessment would be performed.