ATTACHMENT B

OVERVIEW OF THE KEY RESPONSIBILITIES OF THE BOARD, THE AUDIT COMMITTEE AND TOP MANAGEMENT

I. GENERAL OBSERVATIONS

Management is responsible for the operations of the entity. This responsibility includes safeguarding the entity's assets from fraud, waste and abuse and ensuring that the financial information related to the operations of the entity is complete, accurate and adequately disclosed. In the government sector, these responsibilities also include the assurance that the entity is complying with all relevant laws, rules, policies and procedures.

These responsibilities are complicated by the nature of most organizations. Due to their size, complexity, the physical dispersion of their operations and their hierarchical structure, top management may be removed from the day-to-day activities of many of the staff of the entity.

The audit committee is the board's tool for ensuring that top management is effectively managing the entity. The audit committee is the final control, as it were, over top management. Due to their position in the organization, members of top management always have the power to override the controls of the entity. Absent an effective oversight structure, management has little or no constraints. That is where the audit committee comes into play.

Through the oversight of top management, the audit committee also indirectly oversees the operations of the entity.

A common question is how can top management be held responsible for the operations of the entity since there is so much that they cannot know about detailed, daily activities? Similarly, how can a handful of auditors to be able to conduct a complete audit of the entity in a short amount of time, since they cannot possibly have the same understanding of the operations of the entity as its staff and management.

So then, how do auditors and management obtain adequate information about the activities of the entity in order to make reasonable conclusions about the results of the operations and the extent to which the entity's assets are safeguarded, that the entity is in compliance with applicable criteria and that the entity's financial information is correct? The backbone of the entity's operations is an effective system of internal controls. By establishing effective internal controls, management can have assurances that the entity is operating as intended. Auditors can also rely on the internal controls if the controls are operating as designed to provide them with the assurances they need to perform the audit. Of course, there is always a risk that the controls may not be working as planned. So the auditors have to take that into consideration as well during the audit. And management should also take that into consideration in their efforts to ensure that the entity is operating appropriately.

Although many examples of effective controls can be cited— such as pre-numbered receipts, daily deposits and segregation of duties—the real test of whether there are effective internal controls within any particular entity is whether there are any consequences if the controls are violated. If there are not, if staff can disregard, circumvent or override the controls without any reactions, then the controls are a myth. Staff can and will learn very quickly if the controls are real or just words buried in policies and procedures. If employees have an opportunity to commit fraud because there are holes in the controls, then they are well-positioned to perpetrate fraud, waste or abuse. For this reason, it is important to identify mistakes that should have been caught by the controls but were not. Fraud does not begin with an illegal act. It can begin when someone realizes that he or she can make “mistakes” that no one else notices or cares about.

Whether the controls are effective or not is solely under the control of management. Auditors should not have any responsibility for establishing the controls; rather auditors have to remain independent of the establishment and maintenance of the controls. Auditors cannot be expected to critically assess something they have had a hand in creating.

One of the key elements of the internal controls is an effective system of communications among staff and top management concerning the status of the controls. It is through such a process that management can stay abreast of the effectiveness of the controls. For management to be able to obtain the degree of confidence they should have in the controls, they must take affirmative measures to require staff at all levels in the entity to monitor the controls and to advise management at each level of any issues related to the controls. The normal tendency in organizations is for information to be fragmented and to be compartmentalized along structural lines. Typically it is very difficult to have information flowing upward: the classical model of communication in a hierarchy is information flowing from the top down. Only by forcing such information upward can top management know what is going on in the entity.

Clearly the degree to which the audit committee can also have the necessary assurances with regard to the activities of the entity is also dependent on the effectiveness of the controls and on the efficiency and effectiveness of the communication of internal control issues from staff and management of the entity.

Therefore, to a very large degree, effective communication throughout the organization is the key to the success of top management and the audit committee. As might be expected, when fraud, waste or abuse is being perpetrated in the organization, the perpetrator is intent on concealing as much information as possible from auditors and others who might object to his or her actions. The particular issue that is motivating the person to commit fraud is usually not known to others in the organization. Accordingly, full disclosure and open communications such as those described below are the antithesis of fraud, waste and abuse.

II. RISK ASSESSMENT

A. Management's Responsibilities

All organizations, regardless of their size or nature, are vulnerable to fraud, waste and abuse. The management of the agency has the responsibility to safeguard the agency's assets from such dangers and to ensure that the agency's financial information is correct.

The primary way in which the management of the agency should seek to safeguard the agency from these risks is by conducting regular periodic risk assessments. The risk assessment is the responsibility of top management. This is not the responsibility of the audit committee, the agency's internal auditors, or the agency's external auditors.

The risk assessment should be well-documented and adequately broad and detailed. It is the first step in protecting the agency from fraud, waste and abuse. The results of the risk assessment are to be used by management to design appropriate internal controls to mitigate those risks.

Management may utilize internal auditors to assist in the risk assessment, but the use of the internal auditors does not excuse management from their direct responsibility to understand the risk assessment and its implications. And since the internal audit staff will usually be relatively small, management should not use the excuse that the internal auditors have not been able to complete the risk assessment as a reason for it not being done. In fact, under those circumstances it is even more critical that management complete the risk assessment timely.

To whatever degree management may task the internal auditors to assist in the risk assessment, the final assessment has to be made solely by top management. After all, internal audit works for management, not the other way around. It is the individuals in management who are responsible for the overall operations of the agency.

HOW MUCH WORK AND DOCUMENTATION IS ENOUGH?
THE PROCESS OF ASSESSING THE RISK OF FRAUD, WASTE AND ABUSE

1. Although management may not have attempted a formal risk assessment before, the concept of a risk assessment itself should not involve ideas or concepts that are totally unfamiliar to them. After all, management should have the most knowledge about the operations of the entity and should already have an appreciation for the internal and external risks of fraud, waste and abuse that the entity faces. This process should not require management to gain any special education or expertise beyond what they already have. Hence, there should not be an extraordinary level of time and energy expended to get started with the assessment. Although there may be some technical operations in the entity, such as transactions involving the receipt of money and the procurement of goods and services, the assessment stage of the process only requires that management recognize that there is a potential for fraud, waste and abuse in these operations. Management may not understand relatively technical fraud schemes, such as kiting or lapping, but they need to think about the general types of problems that

can occur, such as conflicts of interest in procurement processes, overbillings and theft of funds.

2. The process of assessing the risk is not an activity that is unrelated to the basic responsibilities of management. These efforts should not draw management's attention or efforts away from their other basic responsibilities. The process should assist management in its overall efforts to better lead the organization. Hence, the time spent on the assessment should have value for management and the organization.
3. The extent of the work and the related documentation will depend on the relative size and complexity of the entity. The smaller the entity, the fewer steps that should be required. However, even the smallest entity will have some risks of fraud, waste and abuse. And when the entity is government related, there should be a higher sensitivity to potential fraud, waste and abuse.
4. In conducting the risk assessment, management should attempt to prioritize the risks so that they can focus their initial attention on the greatest risks.
5. In selecting initial transactions and operations to review, management is not required to consider every type of transaction or every aspect of operations.
6. Depending on the nature and circumstances of the organization, perhaps over time subsequent reviews can be performed on a cyclical basis, so that eventually most of the operations are covered. The process should be performed in manageable stages.
7. As an overall statement, the standard that management should apply in performing the risk assessment should be one of reasonableness. For example, the entire risk assessment of a large entity would not necessarily be expected to be completed within the span of one fiscal year. The goal should be quality. And the focus should be on identifying the greatest risks first. The key is getting started, building a sound foundation for future assessments.
8. In identifying the risks, as noted above, management should begin with prior audit findings, ensuring that the corrective actions recommended by the auditors have been fully implemented. This includes proper monitoring and communication of the controls as noted below.
9. The assessments should involve the active participation of staff directly responsible for the affected area, for they should have the greatest practical knowledge about the transactions and activities of the section and should be able to identify related risks.
10. When planning the risk assessments, the relative materiality of the potential risks should be considered. Both quantitative and qualitative materiality should be considered. An example of qualitative materiality is the "three-inch headline" test—how would the potential fraud, if it did occur, look in the headlines of the newspaper? Just how embarrassing would it be for the organization, regardless of the relative amount of money involved?
11. With regard to quantitative materiality, the relative value or amount of the item or transaction susceptible to fraud should be considered. It is unlikely that matters that are truly material, in a strict sense, to the financial statements of the entity, if applicable, or to the financial statements of the state might be misstated. However, if

such a large number was involved in a fraud, the effect would be very damaging. On the other hand, even relatively small amounts may be material, depending on the circumstances, including who has perpetrated the fraud, how easy it would have been to prevent it, whether it was a risk or weakness previously known by management, and the type of transaction involved.

12. It should also be remembered that this measure of materiality is in regard to planning for risk. If fraud is actually discovered, whatever the level of materiality, it needs to be immediately reported to the Comptroller of the Treasury pursuant to Section 8-19-501, *Tennessee Code Annotated.*

13. When planning the risk assessment, the nature of the item subject to fraud should also be considered. For example, cash, by its very nature, is more susceptible to fraud than fixed assets, such as land and buildings.

RISK ASSESSMENT DOCUMENTATION REQUIREMENTS

1. The general test is one of reasonableness under the circumstances.

2. The assessment should be written in a non-technical manner so that interested parties who are not accountants can still understand it.

3. There is no one format that is necessary to use. The key is to have an assessment that is complete enough and clear enough so that staff can read and understand the assessment without having to refer to a lot of other information. The documentation should be logical and provide an overall framework as well as specific information related to the particular risk. It should be dated and signed by the preparer(s) and any reviewers. Overly technical jargon should be avoided, although correct terms should be used, with descriptive footnotes as necessary.

4. The assessment should identify the nature of the transaction or operation in question, for example: cash receipts – skimming receipts, or expenditures – paying for services not received or paying padded invoices.

5. The assessment should also describe the basic condition that gives rise to the risk. In this regard, it might be helpful to begin with present or prior audit findings, particularly repeated findings. Audit findings are written to provide a description of the underlying condition and a discussion of the cause of the condition, the results of the condition, the risks and the steps that would correct the condition. For example, there may be a risk that contracts could be improperly amended resulting in excessive costs for a project, if only one person is responsible for reviewing and approving amendments to the contracts. The risk can be mitigated by requiring at least two individuals to approve any requests for amendments and by limiting the amount of total amendments to a contract without further review and approval by the director of the section.

6. Top management may utilize the expertise of accounting staff and other specialists in developing and documenting the risk assessments. This could include the entity’s internal auditors. In fact, management should seek review of the documented

preliminary risk assessment by such staff before finalizing the work. However, management should not merely assign internal auditors or other technical staff to do the risk assessment for management without direct involvement by management. The whole purpose of the risk assessment is to ensure that top management has taken the steps necessary for them to understand the risks facing the entity and the measures that should be taken to address those risks. At any stage of the risk assessment, if management does not fully understand the comments or observations of technical staff, it is incumbent on management to seek clarification from staff about the information before the risk assessment is finalized. One way to help ensure that management has the appropriate level of understanding and has taken informed responsibility for the assessment is to have management make sure that the documentation of the risk assessment does not have any terms or comments that management does not understand completely. It is through that exercise that management can truly enhance their understanding of the risks facing their entity.

7. The external auditors will be available to provide top management with information about the process of the risk assessment and related issues, consistent with the auditors' professional responsibilities to maintain independence from the role of management and from the prospect of the auditors reviewing their own work.

REVIEW OF MANAGEMENT'S DOCUMENTATION. The auditors will review the risk assessment documentation prepared by management for its adequacy, timeliness, completeness, breadth and clarity. The results of that review will be part of the basis of the auditors' conclusions about the control environment of the entity.

In addition, the documentation will be used by the auditors in planning the nature, timing and extent of any testing the auditors may perform during the audit. Hence, the documentation should be adequate to provide the auditors with a clear picture of the actions and the findings and conclusions of management in meeting their responsibilities.

As a starting point, the risk assessment should thoroughly address issues raised by the auditors in prior audits. In addition, the assessment should reflect management's appropriate concerns for safeguarding the entity from fraud, waste and abuse from internal and external threats. As previously noted, the assessment is to be the work product of management and not internal audit.

B. The Board and Audit Committee's Responsibilities

Although the audit committee is not responsible for the execution of the risk assessment, the audit committee is responsible for reviewing the details of the risk assessment prepared by management. The board, being the body that has ultimate responsibility for the agency, has the duty to ensure that management's risk assessment is adequate, in its documentation, its breadth and its conclusions. The board meets that duty through the efforts of the audit committee. The audit committee should take whatever steps the members of the committee consider necessary to obtain a sufficient understanding of the risk assessment. The audit committee should independently determine that the risk assessment is adequate and appropriate. In exercising this responsibility, the audit committee should meet with top management and personally review the documentation of the risk assessment. Members of the audit committee should formally sign off on the documentation, acknowledging their approval of the assessment, and document both their discussion with top management and their comments about the risk assessment.

REVIEW OF THE AUDIT COMMITTEE'S DOCUMENTATION OF THEIR REVIEW OF MANAGEMENT'S RISK ASSESSMENT. Auditors will review that documentation prepared by the audit committee at the beginning of the audit as part of the auditors' planning of the audit of the entity. The results of that review will be part of the basis of the auditors' conclusions about the control environment of the entity and in considering the nature, timing and extent of any test work the auditors may perform. Hence, the documentation should be adequate to provide the auditors with a clear picture of the depth and breadth of the actions of the audit committee in meeting its responsibilities.

III. INTERNAL CONTROLS OF THE AGENCY (CONTROL ACTIVITIES)

A. Management's Responsibilities

The internal controls of the agency are the primary factors that protect the entity from fraud, waste and abuse. To be effective, internal controls must be well-designed, appropriately implemented and regularly monitored. When the controls are found to be in need of corrective action, that action should be taken as soon as possible.

Designing, implementing and monitoring internal controls are the absolute responsibility of the agency's top management. These matters are not the responsibility of the audit committee. These matters are not the responsibility of the agency's internal auditors, if the agency has internal auditors, or the entity's external auditors.

Management of the agency may assign internal audit staff to assist in their efforts to design and monitor the internal controls. However, management has the primary responsibility for the design and monitoring of the controls. In this regard, monitoring controls is different from testing controls. Internal and external auditors include testing controls during their audits, as appropriate under the circumstances. This testing is specifically targeted to particular issues and particular controls. It is infrequent and limited. It is not intended to provide continuing broad assurance that the controls are designed and operating effectively. Finally, when testing is performed by an auditor, the staff directly responsible for the controls are aware of the auditor's presence and are more likely to make sure the agency's policies and procedures are being followed during the period of the testing.

The monitoring of controls should be an ongoing process. Audits are snapshots of the activities of the entity at a particular point in time or over a relatively short period of time. The real impact of controls is how they work on a regular basis in the entity's day-to-day operations. Controls that might be working on the day that they are tested by the auditors may be abandoned or overridden the next day. Waiting to review and monitor the controls until the next audit period is to ignore the realities involved in safeguarding public assets from fraud, waste and abuse.

The monitoring of internal controls should be the responsibility of all staff, but ultimate responsibility rests with top management. Internal controls should be well-designed and clearly documented in policies and procedures and through appropriate forms and practices. All staff responsible for a particular area in question should understand what the controls are; their significance to preventing and detecting fraud, waste and abuse; and the importance of recognizing when controls are overridden, circumvented or otherwise disregarded. This includes situations in which the "formal written" controls are only theoretical and the real day-to-day operations involve other, unofficial practices. Sometimes controls that seem well-designed in theory are not practical. Rather than stepping forward and advising management that the controls are impractical, staff may just pay them lip service, while doing things contrary to the controls. Sometimes staff complain that the controls may be too rigid to permit the flexibility needed to "get the job done." There is no reason that controls should be that inflexible. More likely, when the controls were developed, there was not a thorough understanding of all of the types of transactions that would be recorded, and/or perhaps new types of transactions or operations have been initiated since the controls were first put into place and the controls have not been adequately amended. Whatever the circumstances, when controls do not "fit" the needs of the staff, they may feel justified in circumventing or ignoring them.

Instead, management should ensure that staff know that they should notify management of the problems with the controls, and the controls should be revisited so that more effective and efficient controls can be implemented.

HOW MUCH DOCUMENTATION OF INTERNAL CONTROLS BY MANAGEMENT IS ENOUGH?

As with the risk assessment noted above, the test should be one of reasonableness. The documentation should be adequate to clearly explain to staff how the transactions and operations in question are to be executed and recorded. There should already be documentation of the major controls currently in place. If not, the documentation of those controls should be a priority. In this regard, issues concerning internal control weaknesses or non-compliance with controls noted during recent audits, and especially repeated findings, should be the starting place.

The standards related to the basic components of internal controls were established many years ago. These concepts should not be new to management. However, the internal and external auditors are available to assist management in understanding any technical internal control issues that they might have.

In reviewing the adequacy of internal controls, management should also use the risk assessment as a starting point. To that end, the documented risks should be directly linked, in writing, with the related controls. Perhaps there are already controls that management feels adequately reduce the risks of fraud, waste and abuse to a reasonable level. In such cases, management should just note that conclusion, clearly describing the connection between the risk and the related controls.

Just because risks have been identified, it should not be assumed that there are no mitigating controls. In fact, it would seem to be more common that the risks that are being formally documented at this time have already been considered by management over the years and have been addressed by controls already in place. Of course, management still has to ensure that the controls are functioning as designed and that they are truly effective to mitigate those risks.

In that regard, management should keep in mind that circumstances do change over time. So rather than presuming that once a risk has been identified and addressed it is not an issue any longer, management should take steps to ensure that the underlying circumstances have not changed. This process would include confirming that the original risk has not changed and that the control is still effective. Manual operations which have been automated would be an example of a situation calling for a reassessment of the risks and controls.

The same considerations related to materiality in terms of risk assessments should be applied to internal controls. Not every transaction or operation requires the same degree and level of controls. In large entities the full implementation of all controls may take extended periods of time, so management should act reasonably in addressing the greatest risks first.

Concerning the use of accountants and other technical professionals, internal controls necessarily involve the understanding and application of professional accounting principles and auditing standards at some level. However, like with any technical aspect of an office, top management ultimately has to accept responsibility for the execution of the operations of the office. Furthermore, the principles underlying internal controls are founded on common sense and practical approaches to preventing fraud, waste and abuse and for ensuring that management's intentions are understood by all staff and are properly carried out. It is not necessary that top management become trained accountants for them to understand the reasoning behind controls. In much the same way, most individuals who exploit weaknesses in internal controls to commit fraud are not accountants either. They simply find practical ways to override or circumvent the controls and wait to see if the system reacts negatively. Put another way, individuals who drive cars don't have to be engineers. But they do have to realize that when "check engine" lights or other gauges indicate there are problems, they need to follow up on them. In fact, the less technical top management is, the more they need to make sure that the controls are designed and documented in a way that makes sense to them and that will "flag" problems.

REVIEW OF MANAGEMENT'S DOCUMENTATION. Auditors will also review the documentation prepared by management supporting the execution of their internal control responsibilities at the beginning of the audit for the same purposes and to the same degree as noted above for the risk assessment.

B. The Board and Audit Committee's Responsibilities

The board as a whole is responsible for appropriate oversight of management. The board should ensure that the audit committee has the duty and powers necessary to keep the board apprised of issues relating to accountability of management and staff of the entity.

The audit committee has two primary responsibilities relative to internal controls:

1. The audit committee is responsible for reviewing the actions of top management in designing, implementing and monitoring the internal controls. This should include a review of the formal policies and procedures that management has communicated to staff informing them of the importance of the individual controls, their need to continually monitor the controls and their responsibility to advise management of situations in which the controls are either not functioning properly or have been circumvented or overridden.

   The audit committee should also ask to see any communications from staff detailing any such situations and review the steps taken by top management to address those issues.

2. The audit committee is also directly responsible for the oversight of top management. In this regard, the audit committee should ensure that there are adequate safeguards in place to prevent top management from overriding the controls. For example, the audit committee should insist on formal policies and procedures that require top management to obtain the approval of the board or the audit committee for transactions initiated by top management that are not otherwise subject to review through the regular internal controls in the agency. Since members of top management are in a position to override the regular controls and perhaps thwart efforts to limit their powers, it is necessary that the controls be at the next level, i.e., with the board. Of course, the board should also ensure that measures are in place to provide staff with the mechanisms to inform the board of any improper actions by top management.

REVIEW OF THE AUDIT COMMITTEE’S DOCUMENTATION. Auditors will also review this documentation prepared by the audit committee at the beginning of the audit for the same purposes and to the same degree as noted above for the risk assessment.

IV. OTHER INTERNAL CONTROL COMPONENTS

Auditing standards establish five components of internal control: the control environment, risk assessment, control activities, information and communication, and monitoring.

This guidance has already discussed risk assessment and control activities (the internal controls).

To be effective, an organization should address all five components. All of the components are interrelated. For example, if management has taken proactive steps to design and implement effective control activities, then they probably have set the appropriate tone at the top. And if the audit committee has appropriately reviewed and approved management’s actions, the board has also set the proper tone at the top.

Still, the proper control environment depends on top management and the board maintaining the proper commitment to accountability and control on a day-to-day basis.

Likewise, the controls should include proper measures for self-monitoring of the controls so that management and the board will be aware of breakdowns of controls, including circumvention of controls. Controls can't be placed into operation and just left on automatic pilot. The controls should be such an integral part of operations that if they break down it will be noticed. In addition, affirmative steps need to be taken to make sure the controls continue to operate over time as originally designed.

If there is proper monitoring of controls, there is a positive control environment.

This guidance has noted that all staff should monitor controls for indications of problems as part of their regular responsibilities. Although these informal actions are very important, management also has the responsibility to establish formal mechanisms to monitor the operation of controls. These steps should include assignment of a specific individual to perform the monitoring, some documentation of the monitoring efforts and results of the monitoring, as well as documentation of the action of the monitor to follow up on exceptions that are noted. The monitoring has to be on a regular basis and performed by someone independent of the activity being monitored. Monitoring is especially important as a compensating control in situations involving inadequate segregation of duties.

For example, if one person has responsibility for writing checks and reconciling the bank statements—a condition that should be avoided—it is imperative that someone else regularly reviews these activities. The reviewer should be aware of the reasonable indications of fraud, waste and abuse, such as checks to cash, missing checks or bank statements, or unusual checks in terms of amounts, payees, dates, sequences or purpose. When the reviewer finds such items, he or she should follow up on them by asking for explanations, with a questioning mindset, seeking supporting information when appropriate. The reviewer should document all of these matters and, if there appears to be a problem, refer the matter to the appropriate management.

Finally, it is important that there be adequate communication and flow of information throughout the various operations and activities of the organization. This is particularly true of organizations with decentralized operations, dispersed over relatively wide geographical areas, or organizations with multiple layers of operations. After all, for an organization to operate efficiently and effectively, there has to be adequate coordination of efforts. Furthermore, the possibility of undetected control impairments increases substantially as the span of operations grows. As with the other interrelated internal control components, the more effective the communication and flow of information are throughout the organization, the stronger the controls will be, in general.

A. Management's Responsibilities

The real test of communication and information is whether management has demonstrated an appropriate commitment to meeting communication and information needs of the organization.

To this end, top management should include clear formal, written instructions to all staff with regard to how staff should report the results of operations and other key information, including circumstances that might indicate fraud, waste or abuse. These instructions should include specific guidance and with regard to possible fraud, waste and abuse, should provide a way for the person providing the information to remain anonymous, if he or she wishes to do so. The guidance should be effectively communicated to all staff.

The communication guidance should also advise staff to timely report issues relating to internal controls as noted above.

Communications of indications of possible fraud, waste or abuse should be made at least one level above the level of the persons suspected of having engaged in the unacceptable behavior. If the behavior involves top management, the person should report directly to the audit committee. In all cases, anyone suspecting fraud, waste or abuse at any level should be able to report these matters directly to the audit committee.

B. The Audit Committee's Responsibilities

The audit committee should keep all of the components of effective internal controls in mind as they review, evaluate, and approve management's risk assessment and internal controls. The audit committee does not have to document specific examples of management's actions which support an appropriate control environment, adequate monitoring or effective communication and information measures in addition to the audit committee's other documented evaluation of management's risk assessment and internal controls. However, the audit committee should note their overall satisfaction with all internal control components in their documented review and should note any shortcomings with sufficient detail to provide adequate follow-up, including the audit committee's recommendations to management for improvements and management's response.

V. A Special Word About Information Technology

Over the years, many agencies have made dramatic changes in the way significant information is obtained, processed, transmitted, maintained or accessed. Every office is dependent upon information technology to one extent or another. Some have virtually paperless systems.

The advancements in information technology present wonderful opportunities for increased efficiency and effectiveness of operations. However, information technology also presents special internal control issues for entities and their auditors.

Auditors obtain evidence about the operations of an entity in two basic ways: testing individual transactions and testing controls over transactions.

There are inherent limitations in both of these efforts. A sample of individual transactions may not contain any problems even though the controls are ineffective. Perhaps the sample size was too small or the particular transactions tested just happened to be the few that were without errors or irregularities. If the auditor concludes based on such a sample that the other transactions are without problems, i.e., that the relevant internal controls are working, the conclusion would be wrong.

When an auditor tests controls, the test is, in general, as of a specific time. The controls may appear to be operating effectively at that time, but they may be overridden, circumvented or otherwise compromised for the rest of the period under audit. Again, if the auditor concludes that the controls are working based on his or her limited work when, in fact, they are not, then that conclusion would also be wrong.

Some advantages of information technology are that the technology permits storage of massive amounts of information and many transactions can be processed in a very short period of time. However, since the details of the processing of the data, including the controls, are not readily visible, being imbedded in software, it is much more difficult for third parties to observe the controls than in a manual system. And if there are flaws in the controls, many more undetected errors can occur in a shorter period of time. Or more fraud can be perpetrated in a shorter period of time, without as much possibility of detection. Further complicating the reliability of automated data is the possibility that without proper controls such as segregation of incompatible duties, someone could change the controls for certain periods of time to remove or impair imbedded controls and then restore the controls later, without detection.

For these reasons, all parties must be particularly sensitive to the need for effective controls over information technology operations, on a consistent basis. Again, the responsibility for the effectiveness of these controls rests with management and the board.

Since top management and the board may not be familiar with the latest technological advances, it is important that they take reasonable steps to put into place competent, ethical technical staff to oversee these activities, and that top management acts reasonably in meeting their overall responsibility for the activities.

All auditors are not necessarily information technology experts either. However, auditors are trained in ways to consider and evaluate controls over computers and computer systems. In addition to reviewing these controls, generally divided into general and application controls, auditors utilize Computer Assisted Audit Techniques, or CAATs, to test the data stored in and processed by computer systems. The good thing about computers is that practically every file in a particular database can be tested without as much reliance on sampling as was required in the past.

For example, if a key requirement for payment of benefits is a social security number, CAATs can probably be designed to test the field that should contain a social security number for each participant in the program. This test would reveal any participants without valid social security numbers.

Such a test would not only identify specific files with problems (substantive testing of details) but would also indicate that the key control, requiring social security numbers before participation in the program, was ineffective.

Top management should take steps to reasonably ensure that their staff over the information technology operations are knowledgeable about the significant risks to the entity's information technology operations and the significance, importance and need for appropriate general and application controls and know how to design and implement effective controls. Top management should also get documented assurances from these staff that those risks have been clearly identified and mitigating controls have been designed and implemented, that they are operating effectively and are being regularly and formally tested, including tests involving appropriate CAATs. These documents should be part of the documentation prepared by management as part of their risk assessment and internal control design and implementation. Management should seek clarification of any terms, comments, or observations they don't understand before adopting the risk assessments and related controls. The audit committee should look for this documentation in their review of management's efforts and document their review and approval of them.

Auditors will review these documents as part of the audit, as previously noted.