Appendix 3A.01 **General Internal Control Questions**

The following questions are designed to help the governing committee evaluate the internal control process. "Yes" answers indicate desirable conditions, and "no" answers indicate potential weaknesses.

I. Control Environment	**YES**	**NO**	**N/A**
1. Are the duties and responsibilities of the governing committee and of management clearly defined and documented in writing?	___	___	___
2. Does the governing committee meet in regularly scheduled meetings, and are clear written minutes kept of all their meetings?	___	___	___
3. Is sufficient information provided to the governing committee in a manner that allows adequate and timely monitoring?	___	___	___
4. Is the governing committee advised of sensitive information, investigations, or improper acts of employees on a timely basis?	___	___	___
5. Does the governing committee take sufficient follow-up action when needed?	___	___	___
6. Do management and the governing committee take measures to minimize the organization's exposure to potentially contentious legal issues?	___	___	___
7. Does the entity have a current approved organization chart?	___	___	___
8. Is the organizational structure appropriate for the entity's size and function?	___	___	___
9. Does top management demonstrate a concern for internal control by performing important internal control activities?	___	___	___
10. Does top management encourage and support compliance with denominational working policies?	___	___	___
11. Does management use conservative accounting assumptions in preparing financial reports?	___	___	___
12. Does management seek outside counsel and adequate discussion when faced with potentially contentious accounting issues?	___	___	___
13. Does management use a conservative approach to the investment of funds?	___	___	___
14. Is the entity free from external influences (e.g., tax regulations, bank loan covenants) that could generate pressure on management to modify normal accounting and reporting policies?	___	___	___
15. Has management established a control environment that minimizes biases that may affect accounting estimates and other judgments?	___	___	___
16. Are background checks made before hiring key employees, and are the results of these investigations adequately considered by management?	___	___	___
17. Are there regular evaluations of personnel performance?	___	___	___

Appendix 3A.01 **General Internal Control Questions**

I. Control Environment (continued)	YES	NO	N/A
18. Does the workload permit management and accounting personnel the time to be alert to the quality of their work?	___	___	___
19. Are controls over the authorization of transactions established at an appropriate level of management?	___	___	___
20. Are there procedures to ensure a smooth transition of duties in the event that key treasury or accounting personnel leave employment?	___	___	___
21. Has a formal code of conduct been adopted, with policies on conflicts of interest, and are employees required to make a declaration of compliance with it?	___	___	___
22. Do accounting personnel appear to have the background, education, and experience appropriate for their assigned duties?	___	___	___
23. Is adequate training provided for new accounting personnel?	___	___	___
24. Do job descriptions exist, listing specific responsibilities for key personnel?	___	___	___
25. Have employee job responsibilities including specific duties, reporting relationships, and constraints been clearly communicated to them?	___	___	___
26. Are accounting personnel required to take mandatory vacations, and are their duties rotated when they are on vacation?	___	___	___
27. Do personnel have a clear understanding of the types of problems that should be reported to management or the governing committee?	___	___	___
28. Are employees encouraged to report suspected improprieties to management or the governing committee?	___	___	___
II. Control Activities			
1. Has management identified risks relevant to the financial reporting process?	___	___	___
2. Has management identified risks associated with safeguarding of assets?	___	___	___
3. Does management have a plan to manage the risks they have identified?	___	___	___
4. If there are risks relevant to financial reporting that management has decided to accept because of cost or other considerations, are the effects considered to be immaterial to the financial statements?	___	___	___
5. Does management or the governing committee take appropriate follow-up action for identified problems or weaknesses in internal controls?	___	___	___
6. Do employees (including management) keep personal accounts and transactions separate from those of the entity?	___	___	___

Appendix 3A.01 **General Internal Control Questions**

II. Control Activities (continued)	YES	NO	N/A
7. Has the entity purchased a fidelity bond covering all employees who handle cash, securities, and other valuable assets?	___	___	___
8. Is the segregation of duties sufficient, given the size and complexity of the organization and treasurer involvement, to avoid incompatible duties within: the accounting function?	___	___	___
computer operations and programming functions?	___	___	___
9. Are budgets approved by the governing committee?	___	___	___
10. Are financial statements prepared at frequent regular intervals?	___	___	___
11. Do management and the governing committee compare actual results with budgets at regular intervals?	___	___	___
12. Are significant accounting estimates reviewed and approved by senior treasury personnel?	___	___	___
13. Are all journal entries approved before entry?	___	___	___
14. Does someone independent of the related accounting function analyze and reconcile significant accounts on a timely basis?	___	___	___
15. Are periodic comparisons made between actual assets and recorded assets?	___	___	___
16. If significant donations or other revenue are received in cash, are there adequate procedures to protect against theft or loss?	___	___	___
17. Are there sufficient procedures to ensure that restricted donations are properly identified and recorded?	___	___	___
18. Are there sufficient procedures to ensure that management monitors compliance with donor-restricted and committee-designated resources?	___	___	___
19. Has management established policies and procedures to accept and utilize comments or complaints from constituents or other third parties?	___	___	___
20. Has the nature of the entity's computer information system been considered in deciding which control procedures to implement?	___	___	___
21. Have appropriate information systems contingency plans been developed to ensure continued operation in the event of a disaster?	___	___	___
22. Are there policies and procedures that limit access of personnel to data, computer equipment, and computer programs?	___	___	___
23. Has management established procedures for authorizing transactions and approving changes to computer programs?	___	___	___

Appendix 3A.02 Questions Related To Computerized Information Systems

The following questions are designed to help the governing committee evaluate internal controls that relate to a computerized information system. Problems that might occur with any computer system include: human errors, hardware or software failures, computer abuse, and catastrophe. "Yes" answers indicate desirable conditions, and "no" answers indicate potential weaknesses.

	YES	NO	N/A
I. Organizational Controls			
1. Is the information systems (IS) department structurally independent of the departments it serves?	___	___	___
2. Are IS personnel prohibited from initiating or authorizing accounting or financial transactions?	___	___	___
3. Are IS personnel prohibited from initiating changes to master files, or are appropriate procedures followed to control such changes?	___	___	___
4. Are reports of changes given to departments that initiated the changes?	___	___	___
5. Are appropriate procedures followed when IS personnel make corrections to errors in data files or software applications?	___	___	___
6. Is there adequate separation of duties between programmers, system administrators, and computer users?	___	___	___
7. Are the duties of IS personnel rotated periodically?	___	___	___
8. Are IS personnel required to take annual vacations of at least one continuous week, and during the vacationing person's absence are their duties performed by other personnel?	___	___	___
II. Access Controls			
1. Is a specific employee assigned the responsibility for IS security?	___	___	___
2. Are there adequate physical controls to ensure that access to computer facilities is restricted to authorized personnel?	___	___	___
3. Are programmers restricted from access to live operations and data files?	___	___	___
4. Are procedures in place to prevent testing of new or revised software applications on live current data files?	___	___	___
5. Are software users prohibited from having access to source code and programming documentation?	___	___	___
6. Is access to application processing parameter databases restricted to authorized personnel?	___	___	___
7. Are software utilities that can alter data or applications adequately controlled, and is their usage logged for subsequent review?	___	___	___
8. Is access control software used for terminals and workstations so that:			
a. Access is limited to specified persons?	___	___	___
b. Individuals have access to only those applications or files that are necessary to perform their duties?	___	___	___

Appendix 3A.02 Questions Related To Computerized Information Systems

	YES	NO	N/A
II. Access Controls (continued)			
9. If passwords are used to control terminal or workstation access:			
a. Are procedures established to determine that those passwords are confidential and unique?	____	____	____
b. Are passwords changed at regular intervals?	____	____	____
c. Are passwords promptly cancelled for terminated employees?	____	____	____
10. When IS personnel are terminated:			
a. Are they released from sensitive duties immediately?	____	____	____
b. Is their access to the IS system suspended immediately?	____	____	____
c. Are their actions appropriately supervised until their departure from the premises?	____	____	____
11. Are there procedures to prevent remote access to the network through dial-up, Internet, VPN, or other means?	____	____	____
12. If confidential or sensitive data is transmitted via public carrier networks, are protection methods (carrier security, encryption, etc.) used to prevent or detect unauthorized access?	____	____	____
13. For internal network traffic, are procedures that are commensurate with data sensitivity in place to provide security over transmission of data across the network?	____	____	____
14. Are intrusion detection systems in place on the internal network?	____	____	____
15. Has all data been classified and has appropriate risk ranking been established to support and provide evidence for network security controls?	____	____	____
16. For centralized data centers, are there appropriate controls over access to system administrator instruction manuals?	____	____	____
17. For decentralized client server systems, are there appropriate education, training, and support materials available over the server for the system administrator and security administrator?	____	____	____
III. Operational Controls			
1. Are schedules prepared and followed for processing of data through specified software applications?	____	____	____
2. Are changes to work schedules appropriately authorized?	____	____	____
3. Are logs used to record system administrator activities?	____	____	____
4. Are system administrators required to report system failures, restart and recovery, or other unusual incidents, and are those reports reviewed by an appropriate official?	____	____	____

Appendix 3A.02 Questions Related To Computerized Information Systems

	YES	NO	N/A
III. Operational Controls (continued)			
5. Are system administrator instruction manuals available to each system administrator?	___	___	___
6. Are there appropriate procedures to monitor system administrator compliance with prescribed operating procedures?	___	___	___
7. Are there appropriate procedures for back-up and storage of software applications and data files?	___	___	___
8. Is there documented background screening of IS personnel?	___	___	___
9. Are periodic security briefings provided for IS personnel?	___	___	___
10. Are there appropriate procedures to prevent test versions of software applications from being run on live current data, and to control such tests when it is necessary to run them?	___	___	___
11. Are there appropriate controls for situations when outside third parties (such as vendors from whom software is licensed) are permitted to sign on to the client's system, for example, to perform problem detection and resolution procedures?	___	___	___
IV. Disaster Recovery and Contingency Planning			
1. Have contingency plans been developed for alternative processing in the event of loss or interruption of the IS function?	___	___	___
2. If contingency plans have been developed, have they been tested for adequacy in the event of a disaster?	___	___	___
3. Is off-premises storage maintained for:			
a. Master files and transaction files sufficient to recreate the current master files?	___	___	___
b. Application software and related documentation?	___	___	___
c. Copies of the contingency plans?	___	___	___
4. Are copies of the backup files for the following items tested periodically to make certain they are usable:			
a. Software copies?	___	___	___
b. Master files?	___	___	___
c. Transaction or transaction history files?	___	___	___
5. Do contingency plans include procedures for replacing employees who may be injured or otherwise unavailable as the result of a disaster?	___	___	___