COMPUTER CONTROLS

ENTITY NAME: _____

SECTION A

INTERNAL CONTROL OBJECTIVES

- Capture, process, and maintain information completely and accurately and provide it to the appropriate personnel to enable them to carry out their responsibilities and to allow the reliable preparation of financial statements.
- Computer operations use correct programs, files, and procedures.
- Program modifications are implemented correctly.
- Access is restricted to authorized personnel.

POTENTIAL ERRORS AND FRAUD

- Unauthorized access to information and programs.
- Application programs that do not meet management's objectives.
- Processing of unauthorized transactions and omitting of authorized transactions.

UNDERSTANDING OF ACCOUNTING SYSTEM

1. How and by whom are the transactions initiated?

_____

_____

_____

2. Describe the procedures, both automated and manual, by which transactions are recorded, processed, and reported from their occurrence to their inclusion in the financial statements.

_____

_____

_____

3. Describe the source documents that support the transactions.

_____

_____

_____

4. Describe the computer media that is used in the processing of accounting information.

5. Describe the documents and reports generated by the accounting system.

6. Describe the accounting processing, records, and files (including how frequently they are updated) that are used to process the transactions, including how transactions are reflected in journals of original entry and in the general ledger.

SECTION B

FURTHER UNDERSTANDING OF CONTROL ACTIVITIES

	Yes	No	N/A
1. Is the IT department independent of user departments?	____	____	____
2. Is there clear segregation of duties of computer programmers and operators?	____	____	____
3. Are IT personnel prohibited from initiating transactions and changes to master files?	____	____	____
4. Are computer operators required to take annual vacations and are their duties rotated periodically?	____	____	____
5. Is access to the computer room restricted to authorized personnel?	____	____	____
6. Are programmers prohibited from accessing production programs, job control language, and live data files?	____	____	____
7. Are computer operators prohibited from accessing source code and programming documentation?	____	____	____
8. Is testing of new or revised programs on live data files strictly prohibited?	____	____	____
9. Are utility programs adequately controlled and their use logged for subsequent management review?	____	____	____

	Yes	No	N/A
10. Are unique and confidential passwords required to use terminals?	____	____	____
11. Are passwords changed at regular intervals and canceled for terminated employees?	____	____	____
12. Do individuals have access only to those programs or files that are necessary to perform their duties?	____	____	____
13. Are there established procedures for documenting new systems and programs, as well as modifications of existing ones?	____	____	____
14. Do system and program development procedures require active involvement by the users?	____	____	____
15. Are system and program modifications subject to appropriate testing, and are test results reviewed and approved by user and IT management?	____	____	____
16. Are schedules prepared and adhered to for processing of computer applications?	____	____	____
17. Are adequate job set-up and execution procedures in place over:			
a. Setting up of batch jobs?	____	____	____
b. Loading online application systems?	____	____	____
c. Loading system software?	____	____	____
d. Input and output media to be used?	____	____	____
18. Are there appropriate procedures for identifying, reporting, and approving operator actions over:			
a. Initial loading of system and application software?	____	____	____
b. System failures?	____	____	____
c. Restart and recovery?	____	____	____
d. Emergency situations?	____	____	____
e. Any other unusual situations?	____	____	____
19. Are logs used to record operator activities, and are they reviewed by appropriate personnel?	____	____	____
20. Are there appropriate procedures for back-up and storage of programs and data files?	____	____	____
21. Are data files physically removed from the facility and placed in a secure remote location (or using online backup)?	____	____	____
22. Are critical data files, systems, and program libraries backed up regularly and stored off-site?	____	____	____
23. Have contingency plans been developed for alternative processing in the event of loss or interruption of the EDP function?	____	____	____
24. Have computers been safeguarded adequately from environmental hazards by:			
a. Keeping them away from smoke and heat?	____	____	____

	Yes	No	N/A
b. Using adequate surge suppressors that meet UL ratings?	____	____	____
c. Maintaining uninterruptible power supplies, when necessary?	____	____	____
25. Are physical security provisions adequate?			
a. Are the office doors locked when not in use?	____	____	____
b. Are keyboard locking devices used when available?	____	____	____
c. If the computer has a built-in password device at “boot-up”, is it used?	____	____	____
d. In high-risk areas, is a cable locking device attached to the desk used?	____	____	____
e. In high-risk areas, are the computer components secured in a way that they cannot be tampered with or stolen?	____	____	____
f. If a modem is used, is it turned off and/or physically disconnected from the computer when not in use?	____	____	____
g. Have all master copies of software been adequately protected and stored away from the computer site?	____	____	____
26. Are software security provisions adequate?			
a. Are passwords used for all important applications?	____	____	____
c. Are passwords secured and not easily visible?	____	____	____
d. Are passwords changed periodically?	____	____	____
27. For all custom-developed programs, does the entity use parallel testing methods before converting to use?	____	____	____