

**AUDIT PROGRAM
CLIENT/SERVER GENERAL CONTROLS REVIEW**

GENERAL BACKGROUND

The purpose of this program is to review and test the controls related to a client/server environment. The objectives in this area are to ensure:

1. Physical assets are adequately safeguarded.
2. Data files and software are adequately secured.
3. Technical and administrative support is adequate.
4. Management support and awareness of the client/server function are adequate.

OBTAIN AN UNDERSTANDING OF THE ENVIRONMENT

To prepare for the detailed audit procedures, obtain an understanding of the following client/server functional areas:

1. Client/server hardware network topology and design (including connections to other networks).
2. System Administrator functions and responsibilities.
3. Work group of users on the client/server.
4. Computer applications used on the client/server.
5. Network software used on the client/server.
6. Organization procedures and standards relating to network design, support, naming conventions, and data security.
7. Management philosophy regarding client/server usage and application.
8. Regulatory environment affecting the client/server environment.
9. User attitude regarding client/server effectiveness.

**AUDIT PROGRAM
CLIENT/SERVER GENERAL CONTROLS REVIEW**

INDEX

<u>Areas of Review</u>	<u>Pages</u>
A. ORGANIZATION AND MANAGEMENT	3-8
B. COMPUTER OPERATIONS	9-14
C. PHYSICAL SECURITY	15-17
D. ENVIRONMENTAL CONTROLS	18-21
E. PROGRAM, DATA FILE AND TRANSACTION SECURITY	22-28
F. SECURITY ADMINISTRATION	29-32
G. APPLICATIONS SYSTEMS DEVELOPMENT AND MAINTENANCE	33-39
H. SYSTEMS SOFTWARE SUPPORT	40-44
I. VENDOR RELATIONS	45-47
J. DATA BASE ADMINISTRATION	48-50
K. HARDWARE AND SOFTWARE INVENTORY MANAGEMENT	51-56
L. TELECOMMUNICATIONS	57-68
M. CONTINUITY OF OPERATIONS	69-74

A. ORGANIZATION AND MANAGEMENT				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Has management approved and documented policies and procedures for: <ul style="list-style-type: none"> a. Approval, purchase or development, use, and documentation of client/server applications and systems software? b. Approval and purchase of client/server hardware? c. Security and confidentiality? d. Classification of applications by risk? e. Backup and recovery guidelines? f. Limited use of outside sources of computerized information, such as bulletin boards and personal files? g. File naming conventions? h. Immediate removal of client/server administration personnel who are terminated due to adverse conditions or performance? 				
2. Has management developed a strategic plan for utilizing client/server technology?				
3. Is the System Administrator required to take vacation?				

A. ORGANIZATION AND MANAGEMENT				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
4. Does an administrative manager reasonably monitor the duties of the System Administrator?				
5. Does the System Administrator have a written job description?				
6. Does a training program exist for the System Administrator and Security Administrator?				
7. Do end-users receive training before being assigned computer processing responsibilities?				
8. Do end-users have problems with accessing and using the application software?				
9. Are end-users notified before a major application or system software change is implemented?				

A. ORGANIZATION AND MANAGEMENT				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Obtain copies of the policies related to client/server development, maintenance, and use. a. Do they include the aforementioned items? b. Have they been reviewed in the last year for currency and changes in technology and business conditions? c. Do the various procedures clearly identify who is responsible for maintaining or performing the function in question?				
2. Obtain a copy of the management-approved client/server strategic plan. a. Does it cover a period of at least two years? b. Has it been reviewed in the last year for currency and changes in technology and business conditions?				
3. On a sample basis, review recent client/server software and hardware purchases. Does the documentation resulting from the purchase comply with written procedures and policies?				

A. ORGANIZATION AND MANAGEMENT				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
4. On a sample basis, select client/server application files and programs. Do they comply with written naming conventions?				
5. Review personnel records to determine if the System Administrator has used all his/her vacation in the last year.				
6. Review personnel records to determine if systems administration personnel have an abnormally high turnover rate in the last three years.				
7. Obtain a copy of the System Administrator job description, verifying that it has been reviewed and approved by management.				
8. Review the job responsibilities of the System Administrator, determining if this person also performed job functions that impair an adequate separation of duties.				
9. Interview the department manager to determine how this person monitors the system administrator activities.				

A. ORGANIZATION AND MANAGEMENT				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
10. Obtain a copy of the training programs for the System Administrator or Security Administrator. <ul style="list-style-type: none"> a. Are they required to participate in the training prior to significant involvement in client/server computing activities? b. Does the training include the appropriate level of information for performing general computing activities, and activities specific to an application or support function? c. Does the training include information regarding security and confidentiality of information, and software copyright laws? 				
11. Interview a sample of client/server end-users to determine their satisfaction with the following: <ul style="list-style-type: none"> a. Level and timing of client/server training provided. b. End-user instructions and documentation. c. Computer response time. d. Computer availability and reliability. e. Application software tools made available to them. f. The planning, timing and adequacy of system updates. 				

A. ORGANIZATION AND MANAGEMENT				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
12. Determine if the end-users sampled in step 11 have successfully retained various basis information regarding client/server operation, i.e., security, problem reporting, basic operation, backup/recovery, etc.				
13. Interview a sample of management and staff who use the reports generated by the client/server. Are they satisfied with the reliability and timeliness of the information?				
SUMMARY COMMENTS – PART A:				

B. COMPUTER OPERATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Are the following client/server operating procedures documented: a. Logon/logoff? b. Backup? c. Hardware maintenance? d. Problem reporting?				
2. Is the System Administrator experienced in and familiar with operation of the client/server facility?				
3. Does the System Administrator have a backup person?				
4. Is the System Administrator assigned responsibility for troubleshooting of client/server problems?				
5. Does the System Administrator maintain a log of: a. Server downtime? b. Device errors?				

B. COMPUTER OPERATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
6. Is the System Administrator assigned responsibility for maintaining the server downtime log?				
7. Is there a documented schedule of operation for cyclical applications, such as payroll and accounts payable?				
8. Does the System Administrator monitor the following: a. Server response time? b. Disk storage space? c. Client/server utilization?				
9. If client/server processing capabilities are limited, does the System Administrator maintain a priority schedule to allow more critical users access before less critical users?				
10. Is the operating system a standard within the business community, and does the vendor support the system, and any customizations?				
11. Are there written schedules and procedures for routine cleaning of the client/server equipment components?				

B. COMPUTER OPERATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
12. Is the System Administrator assigned the responsibility for routine computer equipment cleaning?				
13. Is there scheduled preventive maintenance on the components, either by the System Administrator or by the vendor under a maintenance contract?				
14. Is end-user processing subject to an audit trail, and is this audit trail available for review by the System Administrator?				

B. COMPUTER OPERATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Obtain copies of the client/server computer operations documentation. a. Determine if explanations are adequate for a basic user of the client/server system. b. Determine if the documentation is maintained in a secure location. c. Determine if backup copies are maintained in separate, secure, locations.				
2. Interview the System Administrator to determine if this person is knowledgeable and properly trained.				
3. If available, obtain the client/server application operating schedule. Are key client/server-based financial and operational applications adequately addressed with regard to frequency of processing?				
4. Interview a sample of client/server users and determine if they are satisfied with response time and server availability.				

B. COMPUTER OPERATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
5. During your interview of a sample of client/server users, determine if and when major systems problems have occurred. Match these problems to the System Administrator Problem Log, and ensure that this log identifies how the problems were resolved.				
6. Visually observe the computer equipment within the server facility. Does it appear reasonably clean?				
7. On a sample basis, document manufacturer recommendations regarding cleaning and maintenance of client/server computer equipment. Do written schedules agree with these guidelines?				
8. Interview the System Administrator to ensure this person is knowledgeable about manufacturer requirements and client/server computer equipment in general.				
9. Review the log of server downtime for the last six months. If frequent downtime has been recorded, determine if adequate measures have been implemented to resolve the problem, both for the short term and long term.				

B. COMPUTER OPERATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
10. Interview users of the client/server and ask 1) if they know how to report client/server problems and 2) how often the server has been down in the last six months. Does the server downtime log and procedures adequately reflect the information provided by the users?				
11. If a maintenance contract exists for routine cleaning, verify that the vendor has honored the contract.				
SUMMARY COMMENTS – PART B:				

C. PHYSICAL SECURITY				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Are all client/server hardware devices and documentation located in a secure facility? In particular, the server (keyboard lock and power on password) components should be restricted to the System Administrator. (Note: Other components to include in the physical security review are the wiring closet and cabling.)				
2. Is the server facility reasonably protected against forced entry?				
3. Are keys to the server facility controlled so as to eliminate unauthorized access?				
4. Is the server housing locked or otherwise secured to prevent removal of boards, chips, and the computer itself?				

C. PHYSICAL SECURITY				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Observe the server facility and verify it is physically secured.				
2. Observe the client/server wiring closet and transmission wiring and verify they are physically secured.				
3. Observe the server computer and verify it is secured in such a manner to reduce the risk of removal of components and the computer itself.				
4. Obtain a copy of the key logs for the server room and the wiring closet. Match the key logs to actual keys that have been issued. Are all keys held and assigned to the appropriate people, i.e., System Administrator and support staff?				
5. Select a sample of keys held by people without authorized access to the server facility and wiring closet. Are these keys unable to permit access to these facilities?				
6. Look for client/server operating manuals and documentation that are not properly secured.				

C. PHYSICAL SECURITY				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
SUMMARY COMMENTS – PART C:				

D. ENVIRONMENTAL CONTROLS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Is the power supply to the server properly controlled to ensure that it remains within the manufacturer specifications?				
2. Are the air conditioning and humidity control systems for the server adequate to maintain temperatures within manufacturers' specifications?				
3. Is the server equipment protected from the effects of static electricity, i.e., anti-static rug or anti-static spray, and electrical surges, i.e., surge protector?				
4. Is the server facility kept free of dust, smoke, and other particulate matter, i.e., food?				
5. Is the server facility protected by fire and water detection devices that sound audible alarms?				
6. Are consumption of food, beverage, and tobacco products prohibited by policy in the server facility?				

D. ENVIRONMENTAL CONTROLS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
7. Are backup media, i.e., diskettes, tapes, etc., protected from the following: a. Damage due to temperature extremes b. Effects of magnetic fields c. Water damage				

D. ENVIRONMENTAL CONTROLS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Visit the server facility and verify: <ul style="list-style-type: none"> a. Temperature and humidity are adequate. b. Static electricity guards are in place. c. Electric surge protectors are in place. d. Fire extinguishers are nearby. e. Fire and water detection devices are present and properly operating. f. The area is free of potential flood and water damage. 				
2. Observe the server facility, looking for food and beverage containers and tobacco products in the area and in the garbage cans. Is the area relatively clean and well kept?				
3. Observe the storage methods and media for backup diskettes and tapes, verifying they are protected from environmental damage.				

D. ENVIRONMENTAL CONTROLS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
SUMMARY COMMENTS – PART D:				

E. PROGRAM, DATA FILE AND TRANSACTION SECURITY				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Have client/server data files (software, data, documentation) been classified as critical or sensitive?				
2. Are classified data files adequately protected: a. Against unauthorized access? b. Against unauthorized update? c. From loss, i.e., backed up and stored properly?				
3. Is there an automated client/server security system for restricting, identifying and reporting authorized and unauthorized users of the server?				
4. Does the automated client/server security system deny users' access to client/server components until such time that access has been assigned or invoked?				
5. Are client/server users required to use individually unique logon ID's and passwords to gain access?				
6. Are passwords required to be changed at least twice-a-year, and does the system automatically force these changes?				

E. PROGRAM, DATA FILE AND TRANSACTION SECURITY				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
7. Does the computer system force a password format that inhibits use of easy-to-guess passwords? (Note: This includes requiring passwords to be a least 6 characters and not permitting re-use of a password.)				
8. Are passwords internally encrypted and not displayed on the computer screen when entered?				
9. Is the client/server user's workstation automatically disabled after 3-6 cumulative unsuccessful logon attempts?				
10. Is client/server access based on written management authorization and given on a "need to know/need to do" basis?				
11. Is the management authorization function for client/server user access restricted to only certain designated "data ownership" managers who have responsibility for the reporting content of the computerized data they are responsible for? Are these "data ownership" managers given a regular opportunity to review who can access the computerized data they are responsible for?				

E. PROGRAM, DATA FILE AND TRANSACTION SECURITY				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
12. Is there a standard form for documenting requests for additions, changes, and deletions of client/server logical access?				
13. Are data owners, by policy, required to notify the security administrator in a timely manner of all employee transfers and terminations so security access can be eliminated in a timely manner?				
14. Is access to and use of the client/server monitored by the Security Administrator?				
15. Does a client/server logon session automatically logoff after a short period of inactivity?				
16. Are new users required to use a default password to gain initial access; then is the user immediately required by the system to change their password?				

E. PROGRAM, DATA FILE AND TRANSACTION SECURITY				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Review a sample of sensitive data files to ensure they are properly secured and backed up.				
2. Review a sample of data files labeled as non-sensitive to ensure this classification is correct.				
3. Through reviews of software resident of the client/server and interviews of users, determine if the transaction activity performed is within the scope of the responsibilities of the area and individuals being audited.				
4. Visually verify that the client/server facility, wiring closet, and associated backup diskettes/tapes are in a secured location.				
5. Interview a sample of end-user managers with "data ownership" responsibility to determine if they are aware of their access authorization responsibilities, and have reviewed in the last year who can access the computerized data they are responsible for.				

E. PROGRAM, DATA FILE AND TRANSACTION SECURITY				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
6. Interview a sample of end-users to determine how they were given their initial logon ID and password when they first became system users.				
7. Select a sample of end-users who have recently left the organization or have transferred to other departments, and verify their computer access privileges have been updated or eliminated.				
8. Evaluate a sample of client/server user's access/security profiles to ensure access is appropriate and authorized based on the individual's responsibilities.				
9. Attempt to gain access using a variety of unauthorized logon IDs/passwords. Verify that access is denied and logged.				
10. Logon to and briefly use the client/server. Then, verify that your access and use are properly recorded on the automated activity report.				

E. PROGRAM, DATA FILE AND TRANSACTION SECURITY				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
11. If the client/server logon session automatically logs off after a short period of inactivity, logon to the workstation and visually verify the automatic logoff feature.				
12. Visually search for written passwords in the office and general areas of the computers that utilize the client/server.				
13. Review a sample of client/server access change requests. Does the appropriate management authorize them and is the standard form being utilized?				
14. Obtain a computerized record of those having SUPERVISOR (high-level security access) capabilities, and those having access to the security files and directories. Is this access limited to the Security Administrator and specifically designated, authorized support personnel?				
15. Interview a sample of end-users to verify the interval in which user passwords must be changed.				

E. PROGRAM, DATA FILE AND TRANSACTION SECURITY				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
16. Obtain from the Security Administrator a list of system installed passwords. Verify that they were changed after installation.				
SUMMARY COMMENTS – PART E:				

F. SECURITY ADMINISTRATION				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Is one person (the Security Administrator) responsible for administering logical access to the client/server?				
2. Does an administrative manager reasonably monitor the duties of the Security Administrator?				
3. Does the Security Administrator have a written job description?				
4. Is Security Administrator follow-up of unauthorized access based on written guidelines and adequate to deter further unauthorized use?				

F. SECURITY ADMINISTRATION				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Interview the person responsible for maintaining client/server security to ensure that person: <ul style="list-style-type: none"> a. Is aware of the physical and logical accesses that must be protected. b. Is aware of the need to actively monitor logons to account for employee changes. c. Is knowledgeable in how to maintain and monitor access. d. Is involved in providing end-users with security awareness. 				
2. Interview users to assess their awareness of management policies regarding client/server security and confidentiality.				
3. Obtain a copy of the Security Administrator job description, verifying that it has been reviewed and approved by management.				
4. Review the job responsibilities of the Security Administrator, determining if this person also performs job functions that impair an adequate separation of duties.				

F. SECURITY ADMINISTRATION				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
5. Interview the department manager to determine how this person monitors the Security Administrator activities.				
6. Review a sample of the security reports to: <ul style="list-style-type: none"> a. Ensure only authorized access is occurring. b. Verify timely, evidenced, review of these reports is occurring. c. Look for unauthorized users. If found, determine the adequacy and timeliness of follow-up procedures. 				

F. SECURITY ADMINISTRATION				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
SUMMARY COMMENTS – PART F:				

G. APPLICATION SYSTEMS DEVELOPMENT AND MAINTENANCE				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Are there management authorized policies regarding development and maintenance of client/server application software? Do these procedures require: <ul style="list-style-type: none"> a. Properly authorized user requests? b. User requirements definition? c. Cost/benefit analysis? d. Management authorization of all software changes? e. Detailed testing of all software changes before implementation? f. Backup of old versions of software? g. Logging of all changes and updates to software? h. Notification of affected users prior to implementation? i. Adhering to software licensing and copyright restrictions? j. Procedures for updating of production application software? 				
2. Is the ability to update production application software logically restricted to the Security Administrator, System Administrator, or appropriately authorized support personnel?				

G. APPLICATION SYSTEMS DEVELOPMENT AND MAINTENANCE				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
3. If programming is performed on the client/server, are programmers precluded from updating production software?				
4. If end-users perform programming, are their efforts managed?				
5. In a multi-server or distributed processing environment, are procedures in place to ensure that the versions of the application software used on the various server systems are compatible and consistent across the broad network?				
6. Are the different versions of the application software properly identified and controlled by version numbers?				
7. Is the prior version of updated application software retained on backup files?				
8. Are all program changes subject to evidenced management authorization?				

G. APPLICATION SYSTEMS DEVELOPMENT AND MAINTENANCE				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
9. Are there procedures in place for emergency program updating that prescribe subsequent controlled updating and authorization when time permits?				
10. Are all software updates, including emergency updates, subject to an audit trail? Does the Security Administrator review this audit trail?				
11. Do user manuals exist for all client/server applications?				
12. Are duplicate copies of all user manuals maintained in a separate, secure location?				

G. APPLICATION SYSTEMS DEVELOPMENT AND MAINTENANCE				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Obtain copies of the software update procedures: <ul style="list-style-type: none"> a. Determine if they prescribe that only authorized change personnel, with no programming responsibilities, can perform production software updates. b. Determine if management authorization is required to perform production software updating. 				
2. Obtain a sample of production software update reports, and match to management authorization.				
3. Using the client/server software inventory report obtained earlier, select a sample of application programs (both in-house and purchased systems) and: <ul style="list-style-type: none"> a. Verify management has authorized production updating. b. Verify there are backup copies of the old version of the programs. c. Verify the report identifies the correct version number. 				

G. APPLICATION SYSTEMS DEVELOPMENT AND MAINTENANCE				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
4. If retained, review a sample of client/server software testing documentation to ensure management approved the methods applied.				
5. Select a sample of application programs (both in-house and purchased systems) from the computer and verify: <ul style="list-style-type: none"> a. Users submitted authorized requests for the software. b. Management has authorized production updating. c. There are backup copies of the old version of the programs. d. The changes and updates to the software are being logged and include the correct version number. 				
6. Interview the programmers to determine if they perform production program updating. Also review the programmer job descriptions to ensure production program updating is not one of their responsibilities.				
7. Evaluate a sample of client/server user's access/security profiles to ensure they do not have the ability to update production program libraries.				

G. APPLICATION SYSTEMS DEVELOPMENT AND MAINTENANCE				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
8. In a multi-server or distributed processing environment: <ul style="list-style-type: none"> a. Obtain from a sample of locations a listing of programs used in production. b. Using the client/server software inventory report obtained earlier, select a sample of application programs (both in-house and purchased systems) and verify the correct version numbers are being used at the various processing locations. 				
9. Using the client/server software inventory report obtained earlier, select a sample of applications (both in-house and purchased systems) and verify adequate supporting end-users instructions and documentation.				

G. APPLICATION SYSTEMS DEVELOPMENT AND MAINTENANCE				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
SUMMARY COMMENTS – PART G:				

H. SYSTEMS SOFTWARE SUPPORT				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Are there management authorized policies regarding development and maintenance of client/server system software? Do these procedures require: <ul style="list-style-type: none"> a. Properly authorized user requests? b. Management authorization of all software changes? c. Notification of affected users prior to implementation? d. Adhering to software licensing and copyright restrictions? e. Procedures for updating of production system software? 				
2. Is the ability to update production system software logically restricted to the Security Administrator, System Administrator, or appropriately authorized support personnel?				
3. In a multi-server or distributed processing environment, are procedures in place to ensure the versions of the systems software used on the various server systems is compatible and consistent across the broad network?				

H. SYSTEMS SOFTWARE SUPPORT				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
4. Are the different versions of the systems software properly identified by version numbers?				
5. Is the prior version of updated systems software retained on backup files, or can it be easily obtained from the vendor?				
6. Is virus detection software installed, as a matter of policy, on the server and individual microcomputers (clients)?				

H. SYSTEMS SOFTWARE SUPPORT				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Obtain copies of the system software update procedures: a. Determine if they prescribe that only authorized change personnel, with no programming responsibilities, can perform production software updates. b. Determine if management authorization is required to perform production software updating.				
2. Obtain a sample of production system software update reports, and match to management authorization.				
3. Select a sample of client/server system software and verify: a. Management has authorized production updating. b. There are backup copies of the old version of the programs available on-site or through the vendor.				

H. SYSTEMS SOFTWARE SUPPORT				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
4. Select a sample of systems software from the computer and verify: <ul style="list-style-type: none"> a. Management has authorized purchase and updating. b. There are backup copies of the old version of the programs either on-site or through the vendor. c. The changes and updates to the software are being logged and include the correct version number. 				
5. Evaluate a sample of client/server user's access/security profiles to ensure they do not have the ability to update production system libraries.				
6. If in a multi-server or distributed processing environment: <ul style="list-style-type: none"> a. Obtain from a sample of locations a listing of system software used in production. b. Using the client/server software inventory report obtained earlier, select a sample of system software and verify the correct version numbers are being used at the various processing locations. 				

H. SYSTEMS SOFTWARE SUPPORT				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
7. Obtain the licensing agreement regarding the virus detection software, verifying that it is a site license that permits broad use.				
8. Select a small sample of microcomputers and the server and verify they each have virus detection software installed, updated, and active.				
SUMMARY COMMENTS – PART H:				

I. VENDOR RELATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Is vendor reliability considered before purchasing client/server hardware and software?				
2. Do client/server hardware and software purchase contracts include: a. Statement regarding vendor support and licensing/ownership? b. Dates of delivery? c. Training requirements? d. Technical support? e. Documentation requirements? f. Payment arrangements? g. If appropriate, provisions for upgrades? h. Remedies for the buyer and vendor in case of defaults?				
3. Are hardware and software contracts subject to review by legal counsel before being finalized?				
4. Is a service log maintained to document vendor support servicing?				

I. VENDOR RELATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. On a sample basis, select client/server hardware and software contracts. Determine if the contracts include provisions for: <ul style="list-style-type: none"> a. Vendor support and licensing/ownership b. Dates of delivery c. Training requirements d. Technical support e. Documentation requirements f. Payment arrangements g. If appropriate, provisions for upgrades h. Remedies for the buyer and vendor in case of defaults 				
2. Determine if legal counsel has reviewed the hardware and software contracts.				
3. From the sample of client/server hardware and software contracts, determine if the vendor is reliable. (Note: Such information can be obtained from trade periodicals, financial reporting services such as Standard & Poor's, trade associations, and IS management.)				

I. VENDOR RELATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
4. Obtain the service log and look for software or hardware that has been subject to numerous problems and vendor assisted support. Determine if management and the users can support or justify such activity.				
SUMMARY COMMENTS – PART I:				

J. DATABASE ADMINISTRATION				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Does a technically knowledgeable person have responsibility for Database Administrator?				
2. Do policies and procedures exist to guide development of applications utilizing databases?				
3. Does the Security Administrator administer logical access to the databases?				
4. Does the database management system adequately accommodate concurrent access to the same data element?				
5. Do written procedures exist for recovery of all databases, both from a short-term and long-term interruption of service?				
6. Are database recovery procedures included in the overall client/server disaster recovery plan?				
7. Have database recovery procedures been tested in the last year?				

J. DATABASE ADMINISTRATION				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Interview the System Administrator to determine if this person is knowledgeable about database management.				
2. Interview a sample of end-users of the database systems to determine if they have encountered problems accessing the databases, or if they have noticed database updates that have been altered or suppressed by the system.				
3. Obtain a copy of the client/server disaster recovery plan and verify it includes procedures for restoring the databases.				
4. Obtain documents evidencing tests of restores of the databases.				

J. DATABASE ADMINISTRATION				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
SUMMARY COMMENTS – PART J:				

K. HARDWARE AND SOFTWARE INVENTORY MANAGEMENT				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Is there a complete inventory of all client/server hardware, including the file server, printer(s), modem(s), network interfaces, etc.?				
2. Is there a complete inventory of all client/server software, including application and systems software?				
3. Are there complete records of all client/server software licensing and copyright agreements?				
4. Does the client/server software inventory report identify licensing and copyright restrictions?				
5. Does the client/server software inventory report identify minimal levels of logical access restriction?				
6. Are copies of the client/server software and hardware inventory reports stored at another secure location?				
7. Does the client/server hardware inventory report contain unique identification numbers or model numbers for the various hardware devices?				

K. HARDWARE AND SOFTWARE INVENTORY MANAGEMENT				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
8. Does each client/server hardware component contain an asset number or other ownership identification mark that cannot be removed or altered?				
9. Is there a policy regarding disposal of obsolete or badly damaged client/server equipment? Does the policy require management approval of disposal of equipment?				
10. Is unused equipment stored properly and securely?				
11. Does the organization have written procedures for keeping the client/server hardware and software inventory reports current?				
12. Do organizational policies prescribe that, to ensure compatibility and ease of transfer, only certain types of hardware and software products can be used?				

K. HARDWARE AND SOFTWARE INVENTORY MANAGEMENT				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Obtain a current copy of the client/server hardware inventory report and match, on a sample basis, the inventory report to actual client/server hardware devices. Is all of the client/server hardware present and located in the proper location?				
2. Review the client/server hardware inventory report, on a sample basis, to ensure that only those types of hardware authorized by policy are being used.				
3. Select a sample of client/server hardware devices and match to the current inventory report. Is all the client/server hardware tagged with the appropriate permanent identification mark and reported on the inventory report?				
4. Visit the computer equipment storage room and ensure that all pieces of stored client/server equipment are properly inventoried. Verify that the storage facility is secured.				
5. Obtain a copy of the policy regarding disposal of computer equipment. Has it been reviewed and approved by management in the last year?				

K. HARDWARE AND SOFTWARE INVENTORY MANAGEMENT				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
6. Obtain a current copy of the client/server software inventory report and match, on a sample basis, the inventory report to actual client/server software. Is all of the client/server software present and configured in an authorized manner?				
7. Review the client/server software inventory report, on a sample basis, to ensure that only those types of software authorized by policy are being used.				
8. Select a sample of software resident on the client/server and perform the following: a. Match to the client/server software inventory lists. b. Ensure each is properly authorized and supported by licensing or copyright agreements. c. Ensure the correct version of the software is resident on the system. (Note: This includes in-house and purchased software.) d. Ensure the number of copies of software is use complies with copyright and licensing agreements.				
9. Verify that there are copies of the client/server hardware and software inventory reports at another secure location.				

K. HARDWARE AND SOFTWARE INVENTORY MANAGEMENT				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
<p>10. Obtain a copy of the policy or procedures for maintaining the client/server hardware and software inventory reports and determine the following:</p> <ul style="list-style-type: none"> a. Do the procedures require regular, i.e., annual, updating of the inventory reports? b. Do the procedures identify who is responsible for maintaining the inventory reports, i.e., the System Administrator? c. On the basis of the previous tests and reviews noted above, have the procedures for maintaining the inventory report been adhered to? 				

K. HARDWARE AND SOFTWARE INVENTORY MANAGEMENT				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
SUMMARY COMMENTS – PART K:				

L. TELECOMMUNICATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Are there current network schematics showing telecommunications connectivity throughout the system? (Note: This should include connections to the outside via dial-up lines or the Internet.)				
2. To provide adequate telecommunications line backup, does the office campus have redundant telecommunications lines coming in from opposite sides of the building?				
3. Are logon ID's and passwords required to gain access to the telecommunications network?				
4. Does the security administrator monitor access to the telecommunications network?				

L. TELECOMMUNICATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
<p>5. If using dial-up facilities:</p> <ul style="list-style-type: none"> a. Determine what functions can be performed via dial-up and remote access, and how these functions are protected. b. Does a dial-back feature interrupt telecommunications dial-up connection to the computer and dial back the caller to validate user authority before access to the computer is permitted? (Dial-back can be manual, i.e., the computer operator calls back the user; or automatic, i.e., the computer calls back the user using a computerized list of valid phone numbers.) c. Is access to the internal log of valid telephone numbers permitted computer access secured such that only security administration personnel have access? d. Do the following control features exist: <ul style="list-style-type: none"> (1) Dial-up telephone numbers changed periodically? (2) Dial-up telephone numbers not having the same prefix as the office phone numbers? (3) Dial-up telephone numbers not displayed on modems or terminals? 				

L. TELECOMMUNICATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
6. Once a dial-up connection is made, do logical access controls provide the same restrictions as if the user was using a terminal/workstation from within the organization?				
7. Is there a policy regarding confidentiality of dial-up phone numbers?				
8. Are one of the following control features in place to monitor and detect component failure, communication line errors and intrusions: a. Loop/echo check, to detect line errors? b. Redundancy checks, to prevent system errors, losses, delays, or duplication of data during transmission? c. Parity checks, to check for system errors during transmission? d. Error correction codes, to detect and correct line errors at the receiving location through transmission or use of redundancy code configurations?				

L. TELECOMMUNICATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
9. If there is sensitive data being transmitted over telecommunications lines, is encryption software applied?				
10. Are all telecommunications closets secured from unauthorized access? (Note: In a multi-story building, there should be a telecommunications closet on each floor.)				
11. Are all telecommunications equipment stored in secured locations?				
12. Is there automated or manual program logs maintained to document detection, control, and resolution of abnormal conditions and problems in the telecommunications network?				
13. Is there a trained and qualified network support staff available to troubleshoot telecommunications problems?				
14. Do end-users have planned procedures for dealing with short and long-term interruptions of telecommunications networks?				

L. TELECOMMUNICATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
15. Has telecommunications connectivity been included in any disaster recovery plans?				
16. Does the organization maintain Internet firewalls?				
17. Is a technically competent employee responsible for monitoring the quality and effectiveness of the firewalls?				
18. Is the Internet firewall software secured from unauthorized access?				
19. If the organization transmits confidential or sensitive data over the Internet, are security measures such as encryption in force?				

L. TELECOMMUNICATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
20. Does the organization have Internet policies regarding the following: <ul style="list-style-type: none"> a. "Acceptable Use?" b. Prohibiting downloading of files off the Internet? c. Clear statements of ownership of Internet resources and accounts obtained through the organization? d. Disclaimers of responsibility for employee statements and communications on the Internet? e. Maintaining confidentiality of organization information? f. Security and confidentiality of information on the Internet? g. Repercussions of violating these policies? 				
21. Has legal counsel reviewed Internet usage policies to ensure legality?				

L. TELECOMMUNICATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
22. Are the following automated logs maintained to document efficient and effective use of telecommunications facilities: a. Response Time Reports to identify the time it takes for a command entered by a user at a terminal/workstation to be answered by the computer. (Note: These reports typically identify average, worst and best response times over a given time interval for individual telecommunication lines or systems.) b. Down Time Reports to track the availability of telecommunication lines and circuits.				
23. If the private network is used for e-mail, are there measures, i.e., encryption to protect these transmissions from unauthorized viewing?				
24. If using e-mail, does the e-mail system automatically erase deleted e-mail messages, or is this an option that can be turned on and off. (Note: Some users may not be aware that their deleted messages may be automatically stored in the microcomputer with no computer access restrictions.)				

L. TELECOMMUNICATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
25. If terminals/workstations are installed at customer or vendor sites that have direct or dial-in access: <ul style="list-style-type: none"> a. Is an Off-Site Customer/Vendor Site Terminal/Workstation Program Agreement completed prior to installing the equipment? b. Is this agreement subject to review by legal counsel? c. Are logical access controls in place and being monitored? 				

L. TELECOMMUNICATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Obtain a copy of the network schematics and verify outside connections are noted and reasonably accurate.				
2. If the organization has redundant telecommunications lines coming in from opposite sides of the building, verify they are noted on the schematics.				
3. If the client/server is connected to an outside source through remote access or a dial-up network: a. Attempt to gain access to the client/server through these telecommunications mediums using authorized and unauthorized logon IDs. Determine if the access attempts are logged. b. Determine if the dial-up number has a prefix different from the general office number.				
4. If terminals/workstations are installed at customer or vendor sites that have direct or dial-in access, use the client/server network schematics to determine their location/use.				

L. TELECOMMUNICATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
5. Match a sample of these customers or vendors to their Off-Site Customer/Vendor Site Terminal/Workstation Program Agreements.				
6. Verify the agreements were signed before the equipment was installed and that legal counsel has reviewed these agreements.				
7. Visually observe a sample of telecommunications closets to verify they are secured from unauthorized access.				
8. Visually verify all telecommunications equipment are stored in secured locations.				
9. With the assistance of the system administrator, obtain a copy of a recent telecommunications problem log.				
10. Select a sample of network end-user departments and verify they were provided with plans for dealing with short and long-term interruptions of telecommunications networks.				

L. TELECOMMUNICATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
11. Obtain a copy of the technical disaster/recovery plan and verify it has procedures for reestablishing telecommunications connectivity.				
12. Obtain a copy of the Internet usage policies, and verify they include the issues noted above.				
13. Interview legal counsel to determine if they have had the opportunity to review the Internet usage policies.				
14. Interview the System Administrator to determine if this person is knowledgeable about Internet firewalls.				
15. Ask the System Administrator to identify the date the encryption system (or its most recent upgrade) was installed. (Note: If the encryption system is over two years old, a hacker may be able to compromise computer security.)				
16. Ask the System Administrator to explain the purpose and function of the public and private key encryption algorithm used by the organization.				
17. Obtain copies of Response Time and Network Downtime reports.				

L. TELECOMMUNICATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
SUMMARY COMMENTS – PART L:				

M. CONTINUITY OF OPERATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
1. Is there a complete inventory of all files (operating system, purchased software, in-house developed software, data files) associated with the client/server facility?				
2. Is there a policy regarding updating and maintenance of the client/server file inventory?				
3. For disaster/recovery purposes, have client/server applications been prioritized and scheduled according to their sensitivity and importance?				
4. Are backup copies of all client/server files created at intervals adequate to ensure that they are current?				
5. Are all sensitive client/server applications supported by a written recovery plan?				
6. Are there alternative manual or automated processing procedures in place for end-users for periods when the computer is down?				

M. CONTINUITY OF OPERATIONS				
CONTROL QUESTIONS	YES	NO	N/A	COMMENTS/REFERENCES
7. Is the client/server itself supported by a written disaster recovery plan?				
8. Is a copy of the client/server disaster recovery plan stored off-site?				
9. Have backup files been used to test client/server recovery procedures?				
10. Are client/server backup files stored securely at a site away from the server facility?				
11. Is the server facility protected by insurance coverage?				
12. Is the client/server supported by an uninterruptable electrical power supply?				

M. CONTINUITY OF OPERATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
1. Obtain the client/server inventory list of all files. Does the list agree with the information you obtained when conducting an inventory of client/server software?				
2. Select a sample of client/server software and sensitive data, verifying that they are subject to appropriate backup procedures.				
3. Select another sample of client/server application software and verify: <ul style="list-style-type: none"> a. The applications are supported by a written and authorized recovery plan. b. The applications are prioritized by their level of sensitivity and importance. c. All the sensitive applications sampled have been subject to a test of the backup files. d. The applications are supported by alternative end-user instructions and procedures, both short-term and long-term. 				

M. CONTINUITY OF OPERATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
4. Visit the site where the client/server backup files are stored (hopefully located away from the server facility): <ul style="list-style-type: none"> a. On a sample basis, verify that the appropriate application software, system software, and data files have been properly and timely backed up. Use as your source for the sample the inventory list of software and data. (Note: This may require some technical assistance.) b. Visually observe the backup diskettes and tapes, verifying that they are in the proper storage containers, are not exposed to extreme sunlight or sources of heat, and are not in close proximity to telephones or other devices that generate a strong magnetic field. c. On a sample basis, verify that the backup diskettes and tapes do not contain working files. 				
5. Visually verify a current copy of the client/server disaster recovery plan is stored off-site.				
6. Obtain a copy of the insurance policy that applies to the client/server facility. With the assistance of computer insurance specialists, determine the adequacy of the client/server facility insurance coverage.				

M. CONTINUITY OF OPERATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
7. If an uninterruptable electrical power supply is utilized, determine if the system has been tested in the last year.				
8. Obtain and review a copy of the client/server disaster recovery plan. Does it include provisions for: a. Alternate hardware site? b. Regular testing of the plan? c. A verity of short and long term disasters?				
9. Interview the System Administrator to determine if he/she is familiar with the client/server disaster recovery plans.				
10. Has the client/server disaster recovery plan been reviewed and approved by management in the last year?				
11. Obtain a copy of the most recent client/server disaster recovery test: a. Was the test performed in the last year? b. Were backup copies to production files used to test the recovery process? c. Were end-users involved in the test?				

M. CONTINUITY OF OPERATIONS				
TESTING PROCEDURES	YES	NO	N/A	COMMENTS/REFERENCES
SUMMARY COMMENTS – PART M:				