

<b>Audit Checklist #3 Fifty Steps for Non-IT Auditors</b>				
<b>STEP</b>	<b>YES</b>	<b>NO</b>	<b>N/A</b>	<b>COMMENTS/REFERENCES</b>
1. Have the operational and financial controls over hardware and software additions and dispositions been reviewed?				
2. Are the financing arrangements, i.e. lease vs. purchase for new IT equipment, consistent with the entity's overall goals?				
3. Can all IT equipment be traced to a fixed asset account and conversely can all items recorded in the fixed asset account be physically traced to the actual IT equipment?				
4. Does the entity's internal audit function participate in SDLC (Systems Development Life Cycle) projects?				
5. Does the IT/IS Department use control standards such as job descriptions and organization charts?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
6. Are the IT/IS Department policies readily available, updated, understandable, and reviewed on a periodic basis and distributed to all employees regularly?				
7. Is IT/IS management held accountable for current operating goals, short-term goals, and long-term goals as defined in the entity's strategic plan and are they required to report progress periodically?				
8. Is there monitoring of the number of reports generated (hardcopy and electronic – standard and ad hoc) and of the reports distributed?				
9. Are the entity's records retention policies and requirements known and adhered to?				
10. Is IT/IS system library documentation current and complete?				
11. Is physical access security to the IT/IS hardware resources tested?				
12. Are on-line (logical) access controls to sensitive networks and critical systems tested?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
13. Has a review been conducted to determine how passwords are issued and if they are changed periodically when employees transfer, resign, or are terminated?				
14. Are the controls that exist at remote locations as strong as those that exist at the central processing facility?				
15. Does the entity's internal audit function review how IT/IS detects and corrects errors throughout the processing cycle for critical systems/applications?				
16. Does the entity's internal audit function adjust its audit program based on detected and corrected errors?				
17. When employees give notice of their intent to resign or are terminated, is their access to systems and data immediately revoked?				
18. Is proper control exercised in selecting outside consultants and documenting the respective agreements?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
19. For accountability and control purposes, do the auditors know the location of all sources of input feeding critical systems/applications?				
20. Does the organization have a formal disaster recovery/business continuity plan and are periodic disaster simulations conducted?				
21. Can the auditor determine if, in the event of a disaster or major disruption, the organization has the capability of resuming operations within a reasonable period of time?				
22. Is there a formal procedure for backing up and storing data off-site?				
23. Is the accountability of the IT/IS Department disk and/or tape library inventory procedures tested?				
24. Could unauthorized employees have unrestricted and/or unlimited access to sensitive computerized information?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
25. Is the entity's IT/IS organization reviewed by addressing the following operational audit questions: Are the systems functioning as intended? Is risk and exposure to the systems as minimal as perceived?				
26. Do safeguards exist to prevent access to sensitive information until proper security clearances have been obtained?				
27. Are controls in place to protect access and removal of data held at alternate off-site storage locations?				
28. Are job scheduling overrides controlled at the highest level, properly authorized, and approved?				
29. Do adequate levels of insurance exist in relation to the value of the IT/IS assets, making sure that there is neither omission or duplication?				
30. Can IT/IS management provide the managerial reports necessary for the organization to meet it's short term and long term goals as defined?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
31. Is there a proper segregation of duties between the various functional elements within the IT/IS organization?				
32. Are all changes to production programs properly authorized and documented?				
33. During the systems development process, have embedded modules critical from an audit perspective been considered?				
34. Are emergency instructions written, visible, accessible, updated, and reviewed with new employees?				
35. Are fire safety criteria evaluated regularly and fire drills held periodically?				
36. Where applicable, are negotiable documents safeguarded, sequence numbers accounted for and voided forms clearly marked to avoid misuse?				
37. Are critical documents tested for pre-numbering, accountability, custody, preprinting, turnaround, and cancellation control?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
38. Has a physical inventory of all personal computers (desktops and laptops) been conducted, and compared to the fixed asset records?				
39. Have physical security controls regarding the movement of personal computers (desktops and laptops) been tested?				
40. Do controls exist regarding departmental floppy diskette, compact disc, or other off-line storage accountability?				
41. Do controls exist to monitor and regulate personal computer (desktops and laptops) access to information residing on servers and/or mainframes?				
42. Do organizational policies include standards regarding individual training on personal computers?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
43. Do standards exist which encourage or require personal computer compatibility with other resources within the organization? Are there selected individuals that have the responsibility for enforcing personal computer hardware and software compatibility? Have these individuals issued policies outlining the procedures to be adhered to?				
44. Are all hardware resources protected from electrical power surges?				
45. Are strong user identification procedures employed where the sensitivity of data is an issue?				
46. Has the IT/IS organization completed a quantitative IT/IS risk analysis for attributes such as loss potential, threat probability, and loss expectancy within the past 2 years?				
47. Does an IT/IS steering committee exist, if so, does it have a charter? Does it meet on a regular basis? Conversely, if one does not exist, has the organization considered the benefits which could be derived from one?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
48. Do policies exist regarding licensing agreements and copying licensed software and a policy statement regarding the organization's ethical and legal responsibilities in this area?				
49. Does a properly functioning Quality Assurance function exist within the IT/IS organization?				
50. When it is necessary to transmit data, has the organization considered the possibility of utilizing encryption software?				