

Audit Checklist #1 On-Line Systems Security				
A. GENERAL				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
1. Has an overall security policy, emphasizing the need to keep passwords and sensitive information secure, been developed?				
2. Are employees familiar with the policy?				
3. Are penalties for violating the policy well known?				
4. Has the responsibility and liability of the users, the organization and the network operators been defined in due legal form?				
5. Is access to physical assets and data effectively restricted to only authorized personnel by electronic (logical) and physical controls?				
6. Is there an inventory of network/data communications equipment, including lines, terminals/workstations, routers, modems, firewalls, etc.?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
7. Have written job descriptions been prepared for each major job function and are these descriptions updated when necessary?				
8. Are suspected security violations passed on to a security officer for resolution?				
9. Are the employees periodically retrained to properly apply these security measures?				
10. Is a background check performed on all employees having access to sensitive organizational assets and information?				
11. Is there a back-up facility for the on-line system that is able to respond in the event of an emergency?				
12. Is there proper review of all transaction messages inputted to the system that are unaccounted for, distorted, duplicated or delayed?				
13. Are periodic checks of the network made during normal operation to verify proper operation, detect line/modem errors, terminal operation, etc.?				

B. AUTHENTICATION/AUTHORIZATION				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
14. Is a challenge/response system in use between the user and computer for the purpose of identification and authorization?				
15. Are all users assigned unique user identification codes?				
16. Are passwords assigned to verify users?				
17. Are passwords changed with frequency relative to the sensitivity of the application?				
18. Are multiple levels of passwords used to restrict sensitive functions, similar to multiple levels of government security (i.e., confidential, secret, top secret)?				
19. Are secondary identifiers such as cardkey, fingerprints, or signature verification used to identify and authenticate terminal/workstation users in addition to, or in lieu of, passwords?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
20. Are users sufficiently sensitive to security that passwords are appropriately protected?				
21. Are passwords created using a random method?				
22. If users assign their own password, is there a computer program to review each password to ensure that it is not a copy of the user's name, birthday, social security number, or four or more similar characters?				
23. Does the system prevent a user from selecting a new password that is the same as his/her old password?				
24. Does the system prompt users for change of password at irregular intervals, or better yet, does the system assign new passwords at irregular intervals?				
25. Is there a well defined authority for the responsibility for password changes?				
26. Are passwords printed and distributed in a secure fashion?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
27. Is a security officer responsible for the issuance and maintenance of all passwords? If not, who is responsible and are the controls adequate?				
28. Are procedures for the issuance and maintenance of passwords well documented?				
29. During sign-off, does the system ask the user when his/her next anticipated sign-on will be? Any sign-on before that time period could be reported as a possible violation.				
30. During sign-on, does the system inform the user when he/she last signed off?				
31. Does the personnel or user department notify the appropriate IT individual to remove an employee's ID and password upon termination or transfer? Is this action completed in a timely manner?				
32. Is one-way encryption used to prevent password disclosure should the password table be compromised?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
33. Are passwords masked on both CRT type terminals/workstations as well as printing terminals?				
34. Do terminals/workstations automatically log-off (time-out) after no usage for several minutes?				
35. Are all unsuccessful log-ons recorded, reviewed and monitored for threshold levels?				
36. Does the system prohibit further log-on after "N" unsuccessful attempts? (Usually three)				
37. Does each message contain an identifying message header including: <ul style="list-style-type: none"> ➤ Message number? ➤ Terminal/Workstation ID? ➤ User ID? ➤ Date? ➤ Transaction Code? ➤ End-of-message? ➤ End-of-transmission? 				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
38. Is there a method (sequence number on each message) to account for all messages and identify illegal messages?				
39. Is there a method to prevent inquiry during record updating to avoid incorrect inquiries?				
40. Has message encryption been considered as a means of securing data and passwords during transmission?				
41. Is there one terminal/workstation designated to monitor activity within the on-line system?				
42. Is there a method for creating a log (audit trail) of messages in case of systems failure and/or to monitor users or transactions?				
43. Does the system provide for a restart/recovery procedure to regain communication following a hardware/software failure?				
44. Are passwords and other identification/authentication methods used during the restart procedure to re-establish communications?				

C. TERMINAL/WORKSTATION SECURITY				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
45. Do remote terminals/workstations contain lockable keyboards or physical locks on terminal/workstation on/off switch?				
46. Are terminals/workstations located in a physically secure area?				
47. Is access to the terminals/workstations limited to business hours?				
48. Are there fire detection facilities in the terminal/workstation area?				
49. Is a log maintained of personnel assigned keys or ID cards for terminal/workstation usage?				
50. Are procedures established to ensure that users log-off before leaving a terminal/workstation and that they remove all paper/hard-copy documents which should not be seen by other terminal/workstation users?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
51. Are certain terminals/workstations restricted for input only, or output only, depending on the nature of the business? How is this restriction established and enforced?				
52. Is there a message audit trail so a terminal/workstation user can trace messages sent?				
53. Are log-on, system commands, and on-line transaction documentation manuals labeled as confidential and placed in a secured area when not in use?				
54. Are telephone numbers removed from modems to prevent access to the dial-in telephone number?				

D. SYSTEM SECURITY				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
55. Can the host CPU interrogate a dial-up terminal/workstation and automatically obtain its ID number and verify that the terminal/workstation calling is the same terminal/workstation that says is calling?				
56. Is the on-line system restricted to business hours or are there other scheduled times for the terminals/workstations to come on-line and go off-line?				
57. Is supervisory approval needed to bring a terminal/workstation up outside of scheduled operating hours?				
58. Are individual users restricted to specific functions (i.e. separation of duties)?				
59. Are terminals/workstations programmed to accept only specific transaction types?				
60. Are the day's activities summarized and printed?				
61. In a dial-up network, is the telephone number changed periodically?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
62. Are dial-up lines used in case of leased line failures?				
63. In the event of service interruptions, are there written procedures to follow for restarting the on-line network?				
64. Is a history log maintained of hardware failures to the on-line network?				
65. Does the on-line software log all errors and retransmissions?				
66. Is an individual assigned to review these error logs and notify the security officer if anything unusual is noted?				
67. Is a "call back" to a specific telephone number and reverification of the user ID required?				
68. Do terminals/workstations automatically shut down when abnormal conditions are detected by the host?				
69. Is all test equipment used to monitor the communications network controlled? Is it keylocked? Is there an audit trail of activity?				
70. Are front-end batch controls used to ensure data is entered correctly?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
71. Are back-end control totals used (especially suitable for real-time systems) to ensure the validity of all transactions?				
72. Has character checking (check for blanks, numeric, etc.) as well as field level checking (reasonableness, range, limit tests, etc.) been used to ensure the validity of data being entered into the system?				
73. Is the telephone equipment room secured?				
74. Are terminals/workstations hard wired, therefore eliminating the risk of unknown terminals/workstations gaining access?				
75. Are video display screens shielded to prevent eavesdropping?				
76. Are cables and video display screens electronically shielded to prevent electrical emanations or physical tampering?				
77. Are all security files (password tables, authorization tables) stored in protected files on direct access storage devices and in the computer memory, and are they encrypted if necessary?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
78. If encryption is being used, have controls over the encryption key been developed?				
79. Does the system employ a method of traffic flow security to conceal the presence of valid messages on the line by causing the circuit to appear busy at all times or by encrypting the source and destination addresses of valid messages?				
80. Has the principal of least privilege, i.e., granting the minimum access authorization necessary for performance of required tasks, been implemented?				
81. If using leased circuits, has line conditioning been considered to reduce transmission errors?				
82. Has digital transmission been considered to reduce transmission errors?				

STEP	YES	NO	N/A	COMMENTS/REFERENCES
<p>83. Is a data scope being used by the TP specialists to monitor on-line circuits and equipment? If so:</p> <ul style="list-style-type: none"> ➤ Is it in a secured area? ➤ Does it log entries? ➤ Does it have the capability to enter data onto a line? ➤ Does the unit restrict access to authorized personnel only? 				
<p>84. Are access logs reviewed on a regular basis?</p>				
<p>85. Has the line been checked for active/passive wiretaps?</p>				