Audit Program Guide
Access Controls Audit Program

Budget Hours	Audit Procedures	Done By	W/P Ref.
Background			
	Audit Program Overview		
	1. Access to computer resources should be controlled to protect them against unauthorized use, damage, loss, or modifications. Proper access controls will assist in the prevention or detection of deliberate or accidental errors caused by improper use or manipulation of data files, unauthorized or incorrect use of computer programs, and/or improper use of computer resources. 2. Suggested interviewees for ICQ: a. Documentation Librarian b. System Programming Manager c. Applications Programming Manager d. Director of Information Systems e. Data Base Administrator		
Audit Scope			
	Based on the work performed during the preliminary survey and the assessment of risk, the audit period will cover the operations of [enter client] from [enter date] to [enter date].		
Control Objectives			
	1. Access to Program Documentation 2. Access to Systems Software 3. Access to Production Programs 4. Access to Data Files 5. Access to On-line Systems 6. Access to Data Bases 7. Password Administration 8. Policies for Access Security		
Objective 1: Access to Program Documentation			
	1. Observe the storage location of documentation if it is kept in printed form or determine how access to on-line documentation is restricted. Determine if the documentation is adequately secured. 2. Review documentation check out logs to see if only authorized persons are gaining access to documentation. Determine if checked out documentation is properly logged		

Budget Hours	Audit Procedures	Done By	W/P Ref.
	and can be located. 3. Discuss any audit findings with the Audit Supervisor, Deputy Director and Audit Director. After receiving their approval discuss audit findings with Client management. 4. Summarize and conclude.		
Objective 2: Access to Systems Software			
	5. Interview the person responsible for access to system software. Determine if the methods used to limit access to systems software to authorized persons are adequate. 6. Review documentation check out logs to see if only authorized persons are gaining access to documentation. Determine if checked out documentation is properly logged and if it can be located. 7. Test to see that access to systems software is limited by terminal address. 8. Discuss any audit findings with the Audit Supervisor, Deputy Director and Audit Director. After receiving their approval discuss audit findings with Client management. 9. Summarize and conclude.		
Objective 3: Access to Production Programs			
	10. Interview the person responsible for controlling access to production programs (source and object code) and job control instruction. Determine if passwords and utilities that affect program access are adequately controlled. Also determine if controls are adequate to limit access to only those who need it to do their jobs. 11. Discuss any audit findings with the Audit Supervisor, Deputy Director and Audit Director. After receiving their approval discuss audit findings with Client management. 12. Summarize and conclude.		
Objective 4: Access to Data Files			
	13. Review the procedures for limiting access to data files. Determine if programs not in the production library are adequately restricted from processing against data files and if controls are adequate to restrict access to data files to only authorized persons. 14. Discuss any audit findings with the Audit Supervisor, Deputy Director and Audit Director. After receiving their approval discuss audit findings with Client management.		

Budget Hours	Audit Procedures	Done By	W/P Ref.
	15. Summarize and conclude.		
Objective 5: Access to On-line Systems			
	16. Determine who has access to confidential data. Verify with the owner of the data that these persons have authorization to access this data. 17. Test to see that access to applications, data, or entry and update of transactions is limited by terminal address and hours of operation. 18. For employees that have requested that their addresses and phone numbers not be disclosed, determine if this information is adequately protected from disclosure. 19. Discuss any audit findings with the Audit Supervisor, Deputy Director and Audit Director. After receiving their approval discuss audit findings with Client management. 20. Summarize and conclude.		
Objective 6: Access to Data Bases			
	21. Interview the data base administrator and determine if controls are adequate to restrict access to the data base and data base change utilities. 22. Determine how concurrent access to the same data item is prevented and if it is adequate. 23. Discuss any audit findings with the Audit Supervisor, Deputy Director and Audit Director. After receiving their approval discuss audit findings with Client management. 24. Summarize and conclude.		
Objective 7: Password Administration			
	25. Review the procedures for controlling passwords and determine if they are complete (using 3.4.4 of 1992 EDP Control Objectives as a guide). 26. Review records or interview users to determine when passwords were last changed. 27. In a department where an employee has recently terminated, determine if the employee's password has been deleted and if the passwords of other employees in the department have been changed. 28. Determine how access to password tables is restricted. Determine if access is restricted to only those who really need to access the table. 29. Test to see that there is a limit on the number of unsuccessful attempts to sign on (or login). 30. Discuss any audit findings with the Audit Supervisor, Deputy Director and Audit Director. After receiving their		

Budget Hours	Audit Procedures	Done By	W/P Ref.
	approval discuss audit findings with Client management. 31. Summarize and conclude.		
Objective 8: Policies for Access Security			
	32. Review the policies for access security. Determine if they are complete. 33. Interview the person(s) responsible for access security and determine if they are aware of and follow the policies for access security. 34. Review logs that record accesses. Compare the logs to the list of authorized persons. Determine if access violations are being investigated in accordance with procedures. 35. Discuss any audit findings with the Audit Supervisor, Deputy Director and Audit Director. After receiving their approval discuss audit findings with Client management. 36. Summarize and conclude.		
Effects of Weaknesses			
Access controls are designed to limit access to documentation, files, and programs. A weaknesses in or lack of such controls increases the opportunity for unauthorized modification to files and programs, as well as misuse of the computer hardware. Weaknesses in documentation and/or controls over machine use may be compensated by other strong IS controls. However, weaknesses in systems software, program, and data security significantly decrease the integrity of the system. Weaknesses in this area must be considered in the evaluation of application controls. Notes: Written policies for security over access to automated resources typically address guidelines and responsibilities in the following areas: access to program documentation access to system software access to program and job control instructions access to data files access to applications passwords investigation of access violations To review access controls, the reviewer may need to obtain copies of the automated logs or journals that record/monitor access to the following: program documentation systems software production programs and job control language production data files critical application systems		

Budget Hours	Audit Procedures	Done By	W/P Ref.
password tables Without such documentation, the reviewer may not be able to determine how access to systems software is controlled, in what kind of restrictive area systems software is kept, who are authorized to access and change systems software, and whether certain powerful utilities are being used to circumvent access controls to systems software. Production programs (source and object code) and job control instructions are kept in a restricted area - using secure authentication methods to gain access. Programmers and other unauthorized personnel need to be expressly prohibited from adding, replacing, or deleting production programs. The updating of the production program storage area should be monitored through the use of a report detailing all updates to the production program storage area, and a review of the programs in the production storage area. Someone should be specifically assigned this monitoring responsibility. Production data files also need to be kept in restricted areas. Like production programs, programmers and unauthorized users should be expressly prohibited from updating or deleting production data files. Formal procedures should be in place to limit access to confidential data to authorized persons only.			
Audit Wrap Up			
	37. Complete and index working papers. 38. Prepare a preliminary draft of the audit report. 39. Clear review notes. 40. Forward draft to client and request responses within 10 working days. 41. Incorporate client responses into the final audit report. 42. If requested, schedule and hold exit conference. 43. Quality Control Checklist of the Quality Control Package to be completed by the Deputy Director. 44. Present the audit report.		