Agency **Audit Program - Access**		Initials	Date
	Prepared By		
	Reviewed By		
	W / P Ref		
	Page **1** of **1**		

Procedures	Initials	Date	Reference/Comments
OBJECTIVE - To document the review of the access controls. This program is used to itemize the procedures utilized to allow the auditor to assess the control environment..			
1. Utilize the Access Internal Control Structure Questionnaire to gain an understanding of the control procedures. In completing the ICSQ, include the following: a. results from interviews that further describe the control procedures b. documentation that illustrates the current conditions pertaining to the control procedures.			
2. Summarize control policies and procedures (initial assessment) identified in developing an understanding of the access controls. Include the most significant control policies and procedures that might be tested to provide evidence of their operating effectiveness.			
3. If it is determined to be effective and efficient, design and perform tests which will provide evidence of the operating effectiveness for significant control policies and procedures determined in #2 above.			

Procedures	Initials	Date	Reference/Comments
4. Based upon the above procedures, include any weaknesses on a point disposition sheet. Weaknesses should be discussed with management and finding sheets should be written for reportable conditions.			
5. Include the audit results in an overall memo. Consider the effect of the results, combined with the results of any other ICSQ performed, on the overall control environment.			

		Initials	Date
Agency **Internal Control Structure Questionnaire** **Access**	Prepared By		
	Reviewed By		
	W/P Ref		
Updated: 10/95	Page **1** of **8**		

INSTRUCTIONS NEEDED FOR COMPLETION OF THE QUESTIONNAIRE:

1. The responses to the questions in the ICSQ will be used in gaining and documenting an understanding of the EDP General control structure.

2. Assess the level of control risk for each accounting system or control procedure listed on the ICSQ using the following measures of risk:

   0 - Low Risk
   1 - Moderate Risk
   2 - Slightly Less Than Maximum Risk
   3 - Maximum risk

   Document your justification for the level of risk assessed in the space provided.

3. Cross-reference to flowcharts, narratives, memorandums, etc. that support the control policies or procedures, when applicable.

4. The ICSQ will be maintained in the permanent file rather than the current workpapers. See new permanent file maintenance instructions for further information.

5. The ICSQ can have items added or deleted depending on the particular needs of the current audit.

For clarification or assistance, contact the EDP Audit Specialist Team Coordinator

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #1 - There are written policies for security over access to automated resources.				
1. Have written policies for access security been developed?				
2. Do the policies assign responsibility for the following? a. access to program documentation b. access to systems software c. access to programs and job control instructions d. access to data files e. access to applications f. passwords g. investigation of access violations				
3. Is an automated log or journal used to record/monitor access to the use of the following? a. program documentation b. systems software c. production programs and job control language d. production data files e. on-line application systems f. databases g password tables				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #2 - Access to systems software is controlled.				
1. Is systems software kept in a restricted access area?				
2. Are only systems programmers authorized to access and change systems software?				
3. Are utilities that circumvent access controls restricted and their use monitored? Which utilities? Who monitors?				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #3 - Access to production programs is controlled.				
1. Are production programs (source and object code) and job control instructions kept in a restricted access area?				
2. Are programmers and other unauthorized personnel prohibited from adding, replacing, or deleting production programs?				
3. Is the updating of the production program storage area monitored through the use of the following? a. a report of all updates to the production program storage area b. a review of the programs in the production storage area Who reviews this?				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #4 - Access to production data files is controlled.				
1. Are production data files kept in a restricted access area?				
2. Are programmers and other unauthorized personnel prohibited from updating or deleting production data files?				
3. Are only authorized programs in the production library allowed to process against production data files?				
4. Are there methods in place to limit access to confidential data to only authorized persons?				
5. Is access to production data files monitored? Who monitors?				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #5 - Access to on-line systems is restricted to authorized individuals.				
1. Is access by individuals controlled through the use of the following? a. passwords b. restriction to certain transactions within applications c. restriction to specified hours of operations d. restriction to specific terminals e. other (describe)				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #6 - Access to the database is adequately controlled.				
1. Is a database management system (DBMS) or security software used to prevent access to data by unauthorized individuals?				
2. Are programmers prohibited from changing live data when testing systems?				
3. Are passwords, user I.D.'s or another form of identification used to prohibit unauthorized personnel from accessing data?				
4. Is access to data made only through the DBMS?				
5. Is an automated log or journal produced to identify all accesses to data and who made that access?				
6. Is access to database change utilities controlled through the use of the following controls? a. limiting access to database utilities to authorized personnel b. passwords c. logging the use of utilities				
7. Is a review made of the log to identify unusual entries? Who reviews?				
8. Has a database administrator been appointed?				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #7 - There are procedures for the assigning, monitoring, and deleting of passwords.				
1. Are there written procedures for: a. requesting, approving, and assigning new passwords b. assigning a new password when a user forgets his/her password				
2. Are passwords controlled by the following procedures? a. changing passwords regularly b. changing passwords when an employee changes job responsibilities c. the use of employee exit procedures that include notification of the data processing department for terminating employees' passwords when applicable d. unique assignment to individuals rather than by group e. advising users not to write down passwords f. prohibiting passwords from printing out on the terminal or on reports g. protecting passwords from unauthorized access through encryption of passwords or security over the password table				
3. Is there a limit on the number of invalid access attempts?				
4. Are invalid access attempts identified, logged, and investigated? If so, by whom?				
5. Are there written procedures for investigation of terminal access violations?				
6. Are there written procedures for maintenance and control over passwords?				

Policy/Question	N/A	Yes	No	W/P - Remarks
Circle the level of Control Risk assessed for this Control Procedure: 0 - Low Risk 1 - Moderate Risk 2 - Slightly Less Than Maximum Risk 3 - Maximum risk				RISK ASSESSMENT JUSTIFICATION:

Access Control Procedure Information

CONTROL POLICY #1: There are written policies for security over access to automated resources.

Written policies and procedures for access security should exist. Policies allow the enforcement of security. Users should understand and follow formalized security policies and procedures to ensure the integrity of data, to protect and conserve assets, to protect employees from unnecessary temptation or suspicion, and to protect management from charges of imprudence if compromise occurs.

The auditor should interview the person responsible for security administration. The auditor should obtain and review the security policies and procedures. The Security Administrator should ensure that policies address access to program documentation, to systems software, to programs and job control instructions, to data files, and to applications. Written password policies and procedures for investigation of access violations should also exist. Data owners, or designees, should use automated logs or journals to record/monitor access to:

- program documentation
- systems software
- production programs and job control language
- production data files
- on-line application systems
- databases
- password tables.

The auditor may want to discuss data ownership with a sample of users to ensure that the security and risk implications on policies and procedures have been addressed with them.

CONTROL POLICY #2: Access to systems software is controlled.

Computer systems software should be stored in a restricted area within the computer system. Systems software should be restricted to systems programmers only. Systems programmers need access to maintain systems software. Access should be controlled by user access rules set up in the security software package installed. The security software allows or denies the access and logs all attempts made, authorized or unauthorized. Utilities such as SUPERZAP should also be restricted to system programmers. The utilities can circumvent access control restrictions and use should be recorded and monitored by Security Administrator. Reports should exist that show activity. These should be monitored and reviewed. Unusual or unauthorized activity should be followed up on.

The auditor should gain an understanding from Security Administration on how access to systems software is restricted. Evidence such as security access reports showing restrictions should be obtained and evaluated.

Explanations on discrepancies or unusual access activities should be obtained from Security Administration.

CONTROL POLICY #3 Access to production programs is controlled.

The production programs (source and object code) and job control instructions should be stored in a restricted access area. (datasets and libraries).

Programmers and other unauthorized personnel should be prohibited from adding, replacing, or deleting production programs. Application programmers should only have access to test programs in test libraries. Application programmers should not be allowed to add, replace, or delete production programs. Updates to the production program storage are monitored through the use of reports showing updates to the production program storage area.

The auditor should gain an understanding from Security Administration on how access to production programs is restricted. Evidence such as security access reports showing restrictions should be obtained and evaluated. Explanations on discrepancies or unusual access activities should be obtained from Security Administration.

CONTROL POLICY #4 Access to production data files is controlled.

Production data files containing information should be kept in a restricted area within the computer system. Automated methods should exist that limits access to confidential data to only authorized persons. An application programmer should have access to test data only; they should not be allowed to add, change, or delete production data. Only authorized users should have access to production data. Programmers and other unauthorized personnel should be prohibited from updating or deleting production data files. Only authorized programs in the production library allowed to process against production data files.

The auditor should gain an understanding from Security Administration on how access to production data files is restricted. Evidence such as security access reports showing restrictions should be obtained and evaluated. Explanations on discrepancies or unusual access activities should be obtained from Security Administration.

CONTROL POLICY #5 Access to on-line systems is restricted to authorized individuals.

On-line access to data should be controlled based on need. User identification (Ids) and passwords, restriction to certain transactions within applications, restriction to specified hours of operations, restriction to specific terminals, restriction with on-line regions are typical on-line access controls that should be in place. The auditor should gain an understanding from Security Administration on how access to on-line systems is restricted.

CONTROL POLICY #6 Access to the database is adequately controlled.

Native security with the database software is commonly the method used to prevent access to the data by unauthorized individuals. Programmers should be prohibited from changing production databases when testing new or modified systems should be in place.

Automated logs or journals produced to identify all accesses to data and who made that access should be used. Access to database utilities should be controlled through the use of the following; limiting access to database utilities to authorized personnel, passwords, and the logging of utilities usage (DBMS tools, IBM SUPERZAP).

The auditor should gain an understanding from the Database Administrator on how access to the database is restricted. Evidence of restrictions such as reports and logs should be obtained and evaluated. Explanations on discrepancies or unusual access activities should be obtained from Security Administration and Database Administration.

CONTROL POLICY #7: There are procedures for the assigning, monitoring, and deleting of passwords.

Written security procedures for the requesting, approving, and assigning of new passwords should exist. The understanding of passwords controls should be documented. Comprehensive procedures encompass passwords that:

- are changed periodically by automated procedures
- are changed when an employee changes job responsibilities
- are deleted at the exit procedures that include notification of the data processing department
- are uniquely assigned by individuals rather than by group
- are logged when invalid access attempts are made and monitored.

In addition, policies should advise users not to write down passwords, prohibiting passwords from printing out on the terminal or on reports, and protecting passwords from unauthorized access through encryption of passwords or security over the password table.
The auditor should obtain and review the written security procedures for the maintenance of passwords. Discussion with a selected sample of users should be performed to ensure compliance to procedures. Forms and documents used to approve access and any changes should be obtained and evaluated for authorization.