Chapter IV - Reviewing Information Security

Introduction

Whenever an agency runs critical application systems or maintains sensitive data files, it should have a sound security management structure. A sound security management structure should include a method of classifying and establishing ownership of resources, operational policies, a security organization and resources, user awareness, and security policies.

The agency’s security organization should include an information security administrator. The security administrator is responsible for the overall information security program, particularly the access controls. Access controls are based upon agency information security policies, and they use access control software to enforce the policies.

The access control software (a) authenticates system users, (b) restricts authenticated users to specific access privileges, and (c) reports attempted security violations and sensitive activities for review.

The information security administrator is responsible for running the access control software. Typically, the security administrator or his assistants assign and revoke personal identifiers (logons), and update the security rules to grant persons access to systems, files and transactions according to management's authorizations. The security administrator is also responsible for monitoring the security reports and taking appropriate actions.

The access control software protects both data files and program libraries. In every case, persons should have access to only those data files and programs that they need to perform their normal job duties.

This chapter contains sections covering security administration, conditions for access control, data security and program security. For each of these audit areas, the reader will find an introduction, audit objective, possible controls, suggested audit procedures and comments on reporting findings.

Whenever the financial auditor plans to rely on an application system and tests the operational effectiveness of the application controls, certain critical general controls should also be tested to ensure that the application systems run in an environment that is secure and reliable. These critical general controls usually include security administration, conditions for access control, data security and program security. The financial and EDP auditors should jointly decide which EDP areas to review according to the overall audit objectives.

As a general rule, EDP auditors have responsibility for testing the information security controls because these tests often require the use of technical specialists. Financial auditors may participate in testing these controls to get training and gain experience. EDP auditors are responsible for communicating the results of the testwork to the financial auditors so that they can make any necessary adjustments in the nature and timing of their work. Financial auditors are ultimately responsible for integrating the results of the EDP control tests into the overall audit effort.
Section 1. Security Administration

Security management begins with identifying the risks associated with the data processed by the agency. The appropriate place to begin to identify the risks is by classifying the types of data used by the agency. Classification may be defined as the systematic labeling of data to indicate that a specific set of protective controls should be in place. Data may be classified to satisfy the legal and business requirements for confidentiality, data integrity, and availability. The responsibility for classification rests with the data owner, the individual who is primarily responsible for the completeness and accuracy of the data. Classification of data and resources may be based on sensitivity to destruction, modification or disclosure.

The determination of data ownership is important to a specific system’s security. The data or resource owner normally is responsible for the ultimate use and disposition of the data or resource. Access authority is normally granted by the owner of the data.

The operational policies governing the management of security should focus on the assets at risk. Specific security concerns should be reflected in the agency’s human resources and security policies, even though these policies typically address concerns beyond the normal responsibility of the security function. Employees are a principal security threat and the first line of defense against possible security violations. Therefore, policies should address employee hiring, conditions of employment, responsibilities for security, and termination or transfer.

Responsibility for security should be assigned to a particular department or individual. Depending on the size of the agency, the security department or administrator should have a clearly defined mission statement, placement within the organization that promotes the authority of the position, and adequate training and tools to perform the security function for the agency.

In order for the security program to be effective, it is essential that there is a user awareness program. This may include training to inform personnel of the importance of the information they handle and the legal and business reasons for maintaining its integrity, confidentiality, and availability. Employees should receive documentation describing security policies, procedures, and individual responsibilities. They may be required to sign a specific statement to acknowledge their awareness and acceptance of responsibility for security.

The administrative security policies should set the standards for the agency. Specific procedures should be developed to ensure that the policies are followed. Procedures should address the design of the security structure, the granting and revoking access to the computer system, the granting and revoking access to data and resources, and the reporting and monitoring of security events.

The major risk associated with security management is that the integrity, confidentiality, and availability of information systems data and resources may be compromised.
Audit Objective

The auditor should determine whether the agency has established a reasonable security management program.

Possible Controls

1. The agency has identified a department, function, or individual responsible for security in the organization.
2. The agency has documented security practices and administration procedures.
3. The agency has documented human resource policies that address security concerns.
4. There is a security awareness training program and security brochures or publications that are available to all users of IS data and resources.
5. The agency has documented and uses a data classification methodology and ownership scheme, and periodically reviews for compliance.
6. There is appropriate segregation of duties between the security administration function and the technical support for the computer systems.

Suggested Audit Procedures

The auditor should perform the following procedures, and any others necessary, to achieve the audit objective:

1.1 Determine whether all external access by other organizations, or individuals outside the agency, has been authorized by management.

1.2 Review and evaluate the personnel policies regarding hiring practices, especially procedures for reference checks and background checks. Ensure that they are consistent with the level of responsibility for each job function.

1.3 Review the security education program to ensure that it is active and current. Determine that the technology focus matches that of the organization.

1.4 Review and evaluate the organizational structure, staffing, responsibilities, and training of the data security administration (DSA) personnel. Include the following areas:
   - DSA reporting relationship
   - DSA staff responsibilities
• Security implications and the level of DSA responsibility for software
• Establishment of a formal security policy and management commitment to that policy
• Method for enforcing data and resource protection
• Qualifications and training requirements for DSA personnel

1.5 Review the security function to determine whether the organization and the established reporting relationship allow it to discharge its duties effectively.

1.6 Review, evaluate, and test the procedures established to monitor and control the activity of DSA personnel, especially the following:
• Required security clearances
• Periodic password change requirements and retention periods (use the security software to determine the parameters that have been set)
• Card-key access to security areas
• Criteria for data classification
• Terminal restrictions on DSA activity (use the security software to identify restrictions)
• Restriction on DSA access to production data and resources (use the security software to identify access privileges)
• Approvals and documentation required for the maintenance of security parameters; addition of new users; deletion of inactive, terminated, or transferred users; and maintenance of user and resource profiles
• Procedures for disabling and reinstating users with excessive security violations

Comments on Reporting Findings

Effective security is dependent on a sound security management structure. The level and complexity of the security system should be consistent with the risk associated with the data processed. Written policies and procedures are necessary to document the position of management on security.
Section 2. **Conditions for Access Control**

The most important information security safeguard that each agency has is its access controls. The access control environment consists of the agency's information security policies and procedures, and the access control software. If each of these is functioning effectively, we can conclude that the conditions for access control are adequate to protect the agency's information resources.

The information security policies and procedures should explain each user's security responsibilities, require each user to sign a statement acknowledging his security responsibilities, and prescribe the penalties for security violations. The policies and procedures should also explain when and how persons are granted or denied access to systems, files and transactions.

The access control software may include both vendor-furnished packages, such as ACF2, Top Secret, or RACF, and custom modules built into application systems. To achieve comprehensive security, the agency may need multiple software products. The vendor products and the custom modules may or may not interface with each other, but they will generally work better if they do.

To be effective, an access control system should: (a) authenticate each computer user, (b) restrict access according to security rules, and (c) produce unusual activity or attempted security violation reports for the security administrator.

Authentication of users requires unique personal identifiers (called logons), and confidential passwords that are changed periodically. Without personal authentication, there is no personal accountability. The use of group identifiers, terminal identifiers and file passwords instead of personal identifiers all fail to establish personal accountability.

Security rules should be easy to review. There are at least four kinds of access privileges: (1) read access lets the user view or copy a file without being able to change it, (2) write access lets the user change the contents of a file, (3) delete access lets the user erase a file, and (4) execute access lets the user run a computer program. In order to avoid having detailed security rules for each combination of user, file and transaction, the agency should have a naming convention for its users, files and transactions, and the access control software should permit group rules. This helps keep the security rules easy to review. Very complicated or lengthy security rules are difficult for the security administrator to review, so there is a chance that loopholes will allow unauthorized accesses to occur and remain undetected.

Security reports should identify both unusual activities by authorized users and attempted violations of the security rules by anyone. The access control software should create security reports daily. The security administrator should review the reports when received, and take appropriate corrective action when improper activities are detected.

If authentication, security rules and security reporting are effective, the auditor can conclude that the conditions for access control are satisfactory to protect the agency's data and programs. The actual protection of the data files and program libraries will be reviewed and tested in Section 3, Data Security and Section 4, Program Security.
Audit Objective

The auditor should determine whether the agency policies and procedures and the access control software are adequate to provide the conditions for effective access control.

Possible Controls

1. The agency has a policy that persons should have access to only those computer resources needed to perform their job duties.

2. The agency has a policy that persons with access to computer resources are required to sign a security agreement acknowledging their responsibilities, including not disclosing any security related information such as sharing passwords.

3. The agency uses access control software to protect its critical systems and sensitive data files stored on mainframe computers, minicomputers, local area network servers and personal computers from unauthorized access.

4. The access control software authenticates system users through unique logon identifiers and confidential passwords. Specifically, this includes:

   (A) Management authorizes the user to access its systems and notifies the security administrator in writing or via secure electronic mail.

   (B) The security administrator assigns a unique logon to the user, and notifies the user of the logon and an initial password.

   (C) The user must enter his logon and password to get access to computer resources. The access control system authenticates the user by comparing the logon and password.

   (D) The user changes the initial password immediately and can change his password directly without going through the security administrator.

   (E) When circumstances change, such as when an employee terminates, management promptly notifies the security administrator to revoke or reassign the user's logon.

   (F) The security administrator revokes or reassigns the assigned logon when notified by management. For convenience, the security administrator may suspend rather than delete inactive logons.
5. The access control software protects the confidentiality of passwords:

(A) Passwords must be at least four or five characters long.

(B) Passwords must be changed every thirty to ninety days.

(C) Passwords lock up after a certain number of unsuccessful attempts.

(D) Passwords do not display on terminal screens when entered, and never appear on printed reports.

(E) Passwords are stored only in protected libraries and in encrypted form. No one can view the password file.

(F) Only the security administrator, or his designees, can change passwords. This is only permitted to reset passwords that have locked up.

6. The agency has a naming convention for its computer resources including users, systems, files and transactions, and the information systems department enforces the naming convention.

7. The access control software restricts specific users to specific computer resources including systems, files, and transactions. To accomplish this, the access control software:

(A) Limits the systems, files or transactions that the user can read, write, delete or execute through security rules.

(B) Refers to groups of users, systems, files and transactions through the agency naming convention.

(C) Permits the security administrator to set up user profiles for various job classes to simplify security rule writing.

(D) Denies users access to system resources unless explicitly allowed in the security rules. This is called abort mode.

The opposite condition, where the system grants access to everything unless explicitly denied, is acceptable only for a short period after implementation of new access control software. This is called allow or warn mode.

(E) Limits the user to major computer resources, such as teleprocessing monitors (CICS, TSO), or sensitive functions (Bypass Label Processing).

(F) Has a logging feature to track authorized but sensitive actions. This feature should not be overused or it becomes ineffective and expensive.

(G) Produces reports for the security administrator to review the users and their privileges.
8. The access control software times out and logs off the user after a period of terminal inactivity, perhaps fifteen minutes. The user should reenter his password to resume processing after such a time-out.

9. Management authorizes users to access specific computer resources consistent with their job duties, and notifies the security administrator to assign specific access privileges to specific users in writing or via secure electronic mail. The security administrator establishes access privileges only according to management's authorizations.

10. The access control software limits access according to specific terminals. This control should never be used in place of personal authentication and access control, but may be used as a supplement.

11. The access control software uses file passwords to protect specific data files from unauthorized access. This control should never be used in place of personal authentication and access control.

12. The agency uses additional access controls to authenticate dial-in users and users connecting from other networks. These additional controls include dial-back modems, phone number validation, routing address checking, and special passwords.

13. The access control software absolutely restricts access to sensitive access control privileges (variously called system manager, superuser, security, account, and audit), and methods of bypassing security (non-cancel) to only those persons who need them to perform their job duties.

14. The access control software prints security reports that contain information about sensitive activities by authorized users and attempted security violations by any users. The security administrator or his designees review these reports and take appropriate corrective action.

Suggested Audit Procedures

The auditor should perform the following procedures, and any others, as needed to achieve the audit objective:

2.1 Interview the agency information security administrator, obtain a copy of the agency information security policies and procedures, and inquire about the access control software that the agency uses to protect its critical applications and sensitive information.

2.2 Obtain the agency and information systems department organization charts, including the names, titles and logons of the key personnel, and the duties and responsibilities of the different units.

2.3 Review the information security policies and procedures and verify that they include:
(A) A policy that persons should have access to only those computer resources needed to perform their job duties.

(B) A policy that users are prohibited from sharing passwords with others or disclosing any confidential security related information.

(C) A requirement that persons with computer access must sign a security agreement acknowledging their responsibilities.

(D) Procedures to issue personal identifiers (logons) to new users.

(E) Procedures to grant users access to specific applications, data files and on-line transactions.

(F) Procedures to cancel access privileges in case of employee reassignments or terminations, or other reasons.

2.4 Obtain the agency's file naming convention. Obtain and examine a list of the agency's files and verify that file names conform with the naming convention.

The following procedures should be repeated for each security software system that the agency uses to protect its critical applications and sensitive information

2.5 Verify that users are personally identified when they log on, not through group or terminal identifiers.

2.6 Verify that the software uses confidential passwords to authenticate users, and that the passwords are well controlled.

2.7 Verify that information resources (systems, files and transactions) are referenced according to the agency naming convention, using wildcards or high-level identifiers as appropriate.

2.8 Verify that broad (major systems and functions) and detailed (read, write, delete, execute) access privileges can be differentiated in the rules.

2.9 Verify that the software produces reports for the security administrator that (a) identify the authorized users, and (b) describe the access capabilities of each.

2.10 Verify that the software operates in abort mode, that is, it prohibits access unless explicitly allowed. Verify that the software appropriately times out inactive terminals.

2.11 Verify that the software can log and report sensitive actions, such as non-routine access to data files by systems engineers. Verify that the agency makes use of these reports to monitor sensitive actions without overusing this feature.

2.12 Verify that the software logs and reports all attempted security violations. Verify that the security administrator makes use of these reports to follow up on attempted violations.
2.13 For each access control system that protects the agency's critical applications and sensitive data, obtain copies of all appropriate reports to review the authorized users and their access capabilities. This information will be used in the following two sections.

Comments on Reporting Findings

Generally, vendor-furnished packages provide all the software features needed to achieve the conditions for effective access control. However, custom security modules built into application systems often do not. All of the defects in custom software should be documented so the corrective action will be complete.
Section 3. Data Security

While data is stored in computer systems, it is vulnerable to unauthorized change or use. To protect the data, the agency should use access controls. If the conditions for access control are adequate (see the previous section), the security administrator should use the access control system to restrict access to data files according to job duties and other legitimate needs.

The people who legitimately need access to data include the following:

1. Some users update the data files through the on-line system when processing transactions. This requires update access to the particular transaction screens corresponding with job duties.

2. Other users view the data files on-line while doing business. This requires inquiry access to the particular transaction screens corresponding with job duties.

3. Some users or production control technicians run batch jobs to update the data files. This requires write access to the data files and execute access to the production programs.

4. Programmers, researchers and analysts read or copy the data files for their own purposes. This requires read access to the data files and execute access to the copy programs.

5. Computer operators or production control technicians copy the data files to make backups. This requires read access to the data and execute access to the copy programs.

6. Computer operators or production control technicians restore backup copies of data files to resume processing after a system failure. This requires delete and write access to the data files and execute access to the file management utilities.

7. Database administrators move data from one location to another when physically reorganizing the database. This requires delete and write access to the data files and execute access to the file management utilities.

8. In emergencies, database administrators, computer operators, users or even programmers change the data using powerful editor software to correct unexpected problems. This requires temporary write access to the data files and execute access to the editor software.

Except for the last item, the access control system should permit these persons to do these things as appropriate. The security administrator should have a procedure to grant emergency access when needed, even during second and third shifts.

The access control system should not permit programmers to change data files, especially when testing changed computer programs. The only exception occurs when a system problem corrupts the data, an emergency fix must made, and the programmer is the only person capable of making the fix.
When multiple access control software products are used to protect the data files, the auditor must understand how the products interact. Typically, the computer center provides a vendor-furnished access control system to protect the overall computing environment, and each application system has custom security routines to restrict access to the transaction screens. We test the application system security in Chapter II, Reviewing Application Systems, Section 4, User Access.

For application system security to work, each application user may need write access to the data files in the overall access control system. When this situation exists, the auditor should make sure that the two security schemes are consistently maintained. Otherwise, a user may be able to make unauthorized changes to the data.

Audit Objective

The auditor should verify that stored data is protected from unauthorized change or use.

Possible Controls

1. The agency has a policy regarding to ownership of application systems and data. The policy assigns responsibility for applications to the appropriate user departments. These departments decide who gets access to the systems and data that they own.

2. The agency uses access control software to control access to its applications and data. To be effective, the access control software:
   
   (A) Includes all system users. No one can bypass authentication or security checking except systems engineers responsible for installing the security software itself.
   
   (B) Restricts each user to only those major functions or systems needed to perform his job duties. Users may be restricted to specific application systems, teleprocessing monitors, etc.
   
   (C) Restricts the use of special privileges, such as security administrator and bypass label processing, to those users who need it to perform their normal job duties.

3. The agency adheres to a file naming convention, and the access control system protects all data files associated with the application, including back up and audit trail files.

4. For each application system, the access control system restricts access privileges according to job needs. To be effective, the access control system:
   
   (A) Restricts write access to data files to only those application system users, production control technicians, computer operators and database administrators who need it to perform their job duties.
(B) Restricts delete access to data files to only those production control technicians, computer operators and database administrators who need it to perform their job duties.

(C) Restricts read access to data files to only those persons who need it to perform their job duties.

Suggested Audit Procedures

3.1 Obtain the agency and information systems department organization charts, including the names and titles of the key personnel, and the duties and responsibilities of the different units.

3.2 Interview the agency information security administrator and inquire whether there is a policy regarding ownership of application systems data files. If so, obtain a copy of the policy. Review the policy and inquire whether the security administrator writes security rules in manner consistent with the policy.

3.3 Interview the agency information security administrator about the access control system. Review all of the reports available from the access control system.

3.4 Obtain the security report that contains the valid logons for the system. Scan the logon report for persons who can bypass security checking. Verify that each person with this privilege requires it to perform his normal job duties.

3.5 Scan the logon report for persons with powerful privileges like security administrator and bypass label processing. Verify that each person with these privileges needs them to perform his normal job duties.

3.6 Select a sample of valid logons, verify that each is still employed or otherwise eligible to have a logon, and review the major functions and systems available to each. Verify that the major functions and systems assigned to each person are appropriate for their job duties.

3.7 Identify the names of the critical applications and sensitive data files. Select a sample of critical application data files for testing.

3.8 Obtain the report that contains the detailed security rules for the application systems. Verify that rules exist for the sample of critical application data files.

3.9 Review the rules and identify the persons who have read, write, or delete access to the data files in the sample. Verify that each person with access has a need for it, and that the type of access is appropriate in all cases. In making this determination, be observant for general rules that make specific rules useless.

3.10 Evaluate the authorized users with access to the data, and consider whether any should be logged. If any are logged, determine whether the logs are properly reviewed by management.
Comments on Reporting Findings

It's surprising how many people have authorized access to data files. This makes the application controls important to detect improper actions by authorized users.

Sometimes, information systems staff have access to change data files, and do so routinely. This may indicate that the system has design weaknesses because errors occur frequently that the users cannot correct through the on-line system. When this is the case, we should recommend that the system be changed so that there is no continuing need for the information systems staff to be changing the data.
Section 4. Program Security

Application programs are written in English-like statements called source programs. These source programs are compiled into machine-readable code called object programs. Both source and object programs are stored in separate libraries called the source and object libraries respectively.

Programming involves three steps: development, test and production. Often agencies will have separate source and object libraries for each step. Programmers write new or changed programs in the development libraries. Then supervisors and others review and test the programs in the test libraries. Finally, production technicians run the approved programs from the production libraries.

Throughout this process, the agency must protect its computer programs against unauthorized change and use. Typically, this is what we expect to see:

1. Programmers write new or changed programs in the development source libraries, perhaps the programmers' personal libraries.
2. When the program is ready, the programmer compiles the source program into the development object library. From this library, the programmer runs the program against test data to verify that it is working correctly.
3. After testing the program, the programmer informs his supervisor that the program is ready for review and approval.
4. The programming supervisor, or his designee, copies the source program from the test source library. Here the supervisor reviews the changed lines of source code, and approves the program for further testing.
5. The supervisor notifies the quality assurance, data base administration, and user departments as appropriate that the program is available for testing.
6. A technician recompiles the source program into the object code test library. The reviewing departments then test the object code to determine that it meets the users specifications, complies with agency standards, and interfaces correctly with the agency's databases.
7. When satisfied, the reviewing departments approve the program to run in production.
8. A production control technician moves the approved copies of the source and object code from the development libraries to the production libraries.
9. Finally, only authorized production technicians run production jobs from the production libraries.
10. There will be situations where there is not a separate development and test library. In these instances, similar controls should still be in place.

* * *
Systems software, unlike application software, is usually purchased from vendors. The access control system should protect the systems software libraries so that only authorized systems engineers or vendor personnel install upgrades. Also, the access control system should protect the powerful systems software utilities from unauthorized use.

Audit Objective

The auditor should determine whether the program libraries secure the programs from unauthorized change or use.

Possible Controls

1. There are separate program libraries for development, test and production.
2. The access control system protects the development libraries so that only authorized programmers can change programs in the source library, and compile programs into the object library.
3. The access control system protects the test libraries so that only authorized technicians or supervisors can copy changed programs into the source library and compile programs into the object library.
4. The access control system protects the test libraries so that only authorized reviewers, including the programming supervisor, the quality assurance group, and the database management group can read the programs in the source library or run the programs in the object library.
5. The access control system protects the production libraries so that only authorized technicians or supervisors can copy changed programs into the source library and compile programs into the object library.
6. The access control system protects the production libraries so that only authorized production control technicians can run the programs in the object library.
7. The access control system protects the systems software libraries so that only authorized systems engineers install systems software modifications, and only authorized persons can use the powerful systems software utility programs.

Suggested Audit Procedures

4.1 Interview the information systems manager and inquire about the agency's program library policies and procedures. Obtain the policies and procedures, if written, and verify that there are separate libraries for (1) development, (2) test, and (3) production programs.

4.2 Identify the names of the development, test and production source and object libraries.
4.3 Obtain the report that contains the detailed security rules for the libraries. Verify that rules exist for each of the libraries.

4.4 Review the rules and identify the persons who have read, write, or execute access for the program libraries. Verify that each person with access has a need for it, and that the type of access is appropriate in all cases. In making this determination, be observant for general rules that make specific rules useless.

4.5 Evaluate the authorized users with access to the libraries, and consider whether any should be logged. If any are logged, determine whether the logs are properly reviewed by management.

4.6 Verify that access to change systems software is restricted to only those systems engineers or vendor representatives authorized to make or install systems software modifications.

4.7 Verify that access to execute powerful systems software utilities is restricted to those persons who need it to perform their normal job duties.

Comments on Reporting Findings

To be secure, the program library security should be rigorous. We sometimes find that programmers can make unauthorized changes to programs in either the test or production libraries. Sometimes, programmers or others can run programs from the development or test libraries against the production data files. All program library weaknesses are reportable.