

This section is intended to review compliance with established policy and procedures protecting or securing data and facilities that process and maintain the organization's vital information. The effectiveness of physical security and data security plans, policies, and procedures should be assessed. The examiner should document any findings, especially those that do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*.

## Tier I

### SECURITY ADMINISTRATION AND ACCOUNTABILITY

1. Determine if an overall security administrator has been appointed. Review the role of the security administrator and/or information security personnel to determine their familiarity with the organization's overall security policies and whether they have adequate authority to recommend and implement controls.
2. Review policies and procedures within the security administration function and whether they provide adequate separation of duties and appropriate supervisory review of security system maintenance activities.
3. Determine whether senior management is involved in and supportive of the information security program.

### SECURITY PLAN

4. Review the data security plan and/or policy and assess its adequacy.
5. Determine whether the security plan for the IS operation is compatible with the security plan of the entire organization.
6. Determine whether procedures are in place to update the security plan and/or policy.

### USER EDUCATION

7. Determine if an education program has been implemented to promote user awareness about organization's security policies and procedures and

assess the adequacy of the training program and materials.

8. Determine whether employees certify periodically as to their understanding and awareness of the information security program.

### **PHYSICAL, BUILDING AND CABINET AND VAULT SECURITY**

9. Assess the building's security program and describe the equipment and/or other measures the data facility uses to provide protection.

### **PHYSICAL SECURITY FOR PCS AND DISTRIBUTED DATA PROCESSING ENVIRONMENTS**

10. Describe and evaluate physical security for standalone PCs and distributed data processing environments (e.g., LANs).
11. Determine whether management has based the level of security measures of standalone PCs or other distributed data processing environments (e.g., LANs) on the significance of the applications processed and the potential risks and exposure to the organization?

### **PERSONNEL, DATA FILE MEDIA, AND COMPUTER OPERATIONS SECURITY**

12. Assess the adequacy of physical and operational controls for the computer operations area including:
  - a. Computer room security.
  - b. Personnel safety.
13. Determine whether there are adequate safeguards and procedures in effect to ensure that only authorized persons are permitted in the computer or machine areas and tape/disk file library.

### **HARDWARE AND SOFTWARE INVENTORY**

14. Identify and describe the authority ordering and distribution of hardware and software if not centralized describe the process.

15. Determine if an inventory system is used to record hardware purchase, distribution, and disposal and assess its adequacy.
16. Determine if all software (whether purchased or developed in-house) is accounted for through an inventory system and its assess its adequacy of the inventory system.

#### **DATA AND PROGRAM SECURITY**

17. Describe and assess the adequacy of controls over:
  - a. Operating system commands, programs, and utilities.
  - b. Application system source and object programs and utilities.
  - c. Development and test programs.
  - d. On-line functions, transactions and data.
18. Identify whether levels of access are approved and periodically reviewed by management.
19. Identify whether procedures are in place to address personnel transfers, new hires, and terminations.

#### **TELECOMMUNICATIONS SECURITY AND ACCESS CONTROLS**

20. Describe the types of telecommunications systems used and assess their security features.

#### **TRANSMISSIONS CONTROLS**

21. Determine if controls are in place to protect the confidentiality and accuracy of transmitted data (e.g., parity checks, message authentication, encryption, etc.).

#### **COMPUTER VIRUSES**

22. Identify and describe the measures management has taken to prevent corruption of data or software and to correct problems caused by computer viruses.

**CONCLUSIONS**

- 23. Review the results of work performed in this section and in sections for planning, audit, and management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.
  
- 24. Discuss with management:
  - a. Violations of law, rulings, regulations, or significant internal control deficiencies.
  - b. Recommended corrective action for deficiencies cited.
  - c. Management's proposed actions for correcting deficiencies.
  
- 25. Assign rating (see Chapter 5 for additional information.)
  
- 26. Prepare an index of workpapers for this section of the workprogram.
  
- 27. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include, important facts, findings, examiner conclusions and recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.
  
- 28. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

**Examiner | Date**

---

**Reviewer's Initials**

## **Tier II**

### **SECURITY PLAN**

1. Determine if the security procedures covers:
  - a. Physical protection of the data processing facility.
  - b. Designation and duties of the security officer(s).
  - c. Authorized data and program access levels.
  - d. Requirements for password composition and change procedures.
  - e. Requirements for access via terminals, modems, or computer system interconnection.
  - f. Monitoring and follow-up of security violations.
  - g. LAN and PC security requirements.
2. Determine whether updates to the policy and procedures are distributed to and reviewed by all appropriate personnel in a timely manner.

### **PHYSICAL, BUILDING AND CABINET AND VAULT SECURITY**

3. Determine whether physical security in the data processing operation is coordinated with that of other organization functions.
4. Determine whether visitors to secured areas are required to sign-in and wear proper ID for easy identification.

### **DATA AND PROGRAM SECURITY**

5. Determine how the security system operates and:
  - a. How access levels are granted.
  - b. Whether all access is restricted unless specifically authorized.
  - c. If the password file is controlled (e.g., encryption).
  - d. How security violations are detected and reported.

- e. Who maintains the system and whether there is proper segregation of duties.
  - f. If reports of security file maintenance are reviewed by an individual without maintenance duties.
6. Determine that access levels are commensurate with job assignments, including whether:
- a. Data entry is separate from file maintenance.
  - b. File maintenance is performed at a supervisory level or receives documented supervisory review.
  - c. Individual users are restricted to application files and functions relative to their job responsibility.
7. Assess whether passwords, user ID's and encryption key procedures are adequately controlled for:
- a. The assignment of passwords.
  - b. Changing passwords and ID's on a regular and frequent basis.
  - c. Suppressing passwords and ID's on the video screen and all printed output.
8. Determine whether passwords are required to be alphanumeric or in some other format that is difficult to guess.
9. In a distributed data processing environment, determine whether controls are in place to limit opportunities to transform the data as it moves through various systems.
10. Determine whether sensitive data is adequately controlled (e.g., printouts, removable media, data visible on CRT terminals).
11. Evaluate whether do security control measures include adequate segregation of duties.

**TELECOMMUNICATIONS SECURITY AND ACCESS CONTROLS**

12. Determine whether physical access to system terminals is appropriately controlled by:

- a. Terminal locks.
  - b. A physically secure location.
13. Determine if logical access to system terminals is controlled appropriately by:
- a. User identification.
  - b. Automatic call-back procedures.
  - c. Automatic time-out or log-off.
  - d. Time of day control locks.
  - e. Terminal identification and authentication checks.
  - f. Access exception reporting.
  - g. Security logs.
  - h. Encryption algorithms.
  - i. Automatic logon ID suspension when the number of attempts at accessing the system have reached a specified limit.
14. Determine whether terminals are controlled as to:
- a. What files they can access.
  - b. What transactions they can initiate.
15. Assess whether dial-up phone numbers changed periodically.
16. Assess whether dial-up lines are controlled by either an automatic callback procedure or physical connection (manual intercept) by operations personnel at the data facility.
17. Determine whether reports are generated that record:
- a. Unusual activity.
  - b. Unsuccessful attempts to gain access to the teleprocessing system or applications.
  - c. Teleprocessing network problems/statistics.

- 18. Determine whether exception reports are reviewed regularly by management or data security personnel for follow-up action.

**COMPUTER VIRUSES**

- 19. Identify the frequency with which virus identification programs are run and updated.
- 20. Proceed to Tier I Conclusions.

**Examiner | Date**

---

**Reviewer's Initials**