ISSUES IN ACCOUNTING EDUCATION
Vol. 18, No. 3
August 2003
pp. 291–306

Evaluation of Network Operating System Security Controls

Cheryl L. Dunn, Gregory J. Gerard, and James L. Worrell

ABSTRACT: Systems and financial statement auditors are often responsible for evaluating compliance with system security controls as part of their annual audit procedures. This assignment provides a practical learning experience that relates your course material to actual tasks practitioners perform. You are provided with simulated data from a realistic company example and are asked practitioner-relevant questions covering a variety of issues related to network operating system access. Monitoring and limiting network operating system access and mitigating the related risk is crucial since any application (including accounting applications) can be accessed, and potentially compromised, through the network operating system.

Data Availability: Student feedback data are available upon request from the first author. Data files to complete the assignment are available on the *Issues in Accounting Education* Teaching Notes website.

INTRODUCTION

With the advent of computer-based accounting and business information systems, the need for evaluating controls surrounding the information systems infrastructure has become critical. Because financial statement auditors render opinions based on information and testing performed against data extracted from client accounting systems (in the form of reports and system-generated financial statements), controls underlying these systems must be evaluated. Without adequate system controls, auditors cannot rely on the integrity of the information generated by the system, nor can they perform an effective audit. Effective system control evaluation requires audit professionals who comprehend information systems. Statement of Auditing Standards (SAS) No. 94 (Auditing Standards Board 2001) stipulates that practitioners must gain an understanding of the client's internal control structure as part of the audit-planning phase. SAS No. 94 emphasizes the necessity to understand how an entity's use of information technology affects audit-relevant risks.

Because the term "risk" has multiple definitions, it is important that we clarify our use of the term for this assignment. We define risk as the possibility of loss or damage. The internal controls over an entity's information systems are a vital component of the internal control structure, particularly for those systems that store and process financial transactions. Auditors utilize their assessment of the client's internal control structure to assess their level of controls reliance. Controls reliance is the amount of "faith" or reliance that the auditor is willing to place on the internal control structure to

Cheryl L. Dunn and Gregory J. Gerard are both Assistant Professors at Florida State University, and James L. Worrell is Senior Information Technology Internal Auditor, IT Internal Audit, Raymond James & Associates.

We thank reviewers and participants of the American Accounting Association's Information Systems Section 2002 Midyear Meeting, two anonymous reviewers, the associate editor, Tom Hall, and editor, Tom Howard, for their valuable input on this instructional resource.

prevent, correct, or detect material misstatements in the financial statements. As such, assessing the strength of the client controls over the information systems influences the auditor's assessment of the internal control structure as a whole. For example, if an auditor's preliminary testing of controls indicates a strong control environment, then the auditor may be able to reduce the amount of substantive testing.

One type of information system control auditors need to consider is logical security over systems, programs, and data. SAS No. 94 specifically mentions the risk associated with a lack of control at a single entry point to a system, which compromises the integrity of the entire database, and potentially results in improper changes to or destruction of data. The network operating system (NOS) is typically the first layer of security in controlling user access from a logical security perspective, especially in a distributed system. The NOS controls user identification, authentication, authorization, and many security and permissions settings for all users and resources on the network. In user identification, the user tells the NOS who he or she is. The NOS authenticates the user by mapping user-supplied credentials, such as user IDs and passwords, to a centralized user store of networked systems. The NOS then authorizes the user to perform various functions (such as read data, change data, delete data, or execute programs) based on stored user and group settings established by the network administrator. Thus, it is important for auditors to understand the controls surrounding the NOS and their effectiveness.

Although individual application-level security usually controls what functions a user can perform within applications, poorly designed or ineffective NOS controls may allow data to be manipulated outside the applications, thereby violating the confidentiality, integrity, and availability of the underlying information. Keep in mind that evaluation of NOS security controls is only a part of the testing auditors need to do to determine overall control risk. Auditors also need to examine clients' specific application controls, reconciliation procedures, and monitoring controls. However, failure to consider NOS security controls may lead to unfounded reliance on the application, reconciliation, and monitoring controls. To this end, the audit methodology of most large public accounting firms requires a review of the general computer controls as a component of assessing control reliance at more than "low." The general computer controls review should include an assessment of the controls surrounding the NOS. In most large financial statement audits, trained information technology auditors are engaged to review the controls over the NOS that will be examined in this exercise, and also perform tests to detect any security weaknesses in the NOS. Such testing would examine applicable service packs and security updates installed, system configurations, and network connections.

Unauthorized access to data is a major risk faced by enterprises. News groups, discussion forums, and best-selling books such as *Hacking Exposed* (McClure et al. 2001) have made it relatively easy to gain unauthorized access to corporate information resources. Bugtraq and similar websites publish frequent vulnerability reports to expose weaknesses in various operating system and application software packages. Therefore it is imperative for organizations to keep abreast of patches, updates, and proper system settings. To ensure adequate controls at every level of the information technology infrastructure, public accounting firms and corporate internal audit divisions are increasingly hiring information technology auditors and specialists.

This assignment utilizes the Windows NT™ Server operating system as a facility for illustrating a subset of the types of tests that auditors perform when auditing a NOS. Windows NT™, created by Microsoft Corporation, is popular in client/server systems and can run on multiple hardware platforms. Popular competing network operating systems include UNIX and OS/2. Auditors use various utilities to extract security and system access data from the NOS for audit test work. The output from these utilities vary across competing operating systems as to the format and labels used to describe the fields, however, similar tests are relevant for examining the controls over any NOS. In other words, once you understand how to perform audit procedures on Windows NT™, that same knowledge applies to other NOSs such as UNIX. You are encouraged to focus more on the types of tests that are performed and the implications of those tests, and less on the format of the data extracted by the utility. In the future, newer NOSs will emerge, but the methodology for auditing a NOS will likely remain fairly constant. You should gain increased understanding of the following concepts from completing this assignment:

- Risk assessment and evaluation of internal controls in general
- Risks associated with unauthorized access to data via network operating systems
- Technology tools used to assist in conducting audits
- Utilities used to extract security and system access data from network operating systems
- Security system specialists and their roles in conducting audits

OVERVIEW

You are now asked to put yourself in the role of a new staff auditor who is assigned to the audit engagement for XYZ Corp. and perform user- and group-level tests as described in the following pages.

Your firm has recently acquired XYZ Corp. as a new audit client. As part of your audit methodology, you are asked to review the general computer controls in place at XYZ to determine the control risk that the audit team will assess. Your part of the project will focus on the Windows NT™ network operating system access controls.

A team of security specialists has conducted a review of the data processing center and has documented the physical security in place at XYZ. The team followed your audit firm's typical procedures and ran an extraction utility against the main authentication server to extract user and group information. The main authentication server is the computer that houses the user identification, authentication, and usage statistics. In a Windows NT Server environment, this computer is called the Primary Domain Controller (PDC). A domain controller is a server that maintains information regarding system users, system resources, and various relationships between users and resources. For example, it controls which users are allowed to access a particular application. In Windows NT™, a domain controller can be the primary domain controller (PDC) or a Backup Domain Controller (BDC). A PDC manages and provides access to the master user database. With a PDC, users log on to just one domain and have access to resources located on many different servers. One or more servers can be a BDC that contains a copy (or copies) of the PDC database. In addition to serving as a backup, the BDC can help manage network traffic. The reason the extraction utility was run against the PDC is that the PDC is the central repository for all user authentication and account/audit information.

For a Windows environment such as that at XYZ Corp., the audit script many auditors prefer is DumpSec designed by Somarsoft. DumpSec is a software program that performs a security audit of Windows NT™. It allows an auditor to obtain a list of user attributes, group memberships, and some system information such as password policies, audit policies, operating system version, hardware types, shared drives, and printers. This is quite beneficial given the complexity of networked systems. This utility is available free of charge at http://www.somarsoft.com (Somarsoft 2001) and is used by many security and audit professionals. Because hackers can also use this tool for malevolent purposes (e.g., to find out which user accounts have access to various applications and to determine password information to make it easier to hack into the system), auditors must consider the risks to companies that result from noncompliance with recommended system security control policies. Your instructor has provided you with the following items, resulting from the data extraction, to facilitate your testing:

- From DumpSec:
  - User dump text data file (casestudyusers.txt)
  - Group dump text data file (casestudygroups.txt)
  - Policy settings text data file (policyextract.txt)
- From Client Documentation:
  - Organization Chart (see Figure 1)
  - Corporate Password Policy (see Figure 2)
- From Our Firm's Toolkit:
  - A database shell that contains empty user and group tables into which you should import the user and group data from the text data files. The database shell also includes queries designed to help you answer the questions in the user account testing and group account testing sections (xyzcase.mdb).

The tests you are asked to conduct in order to assess the effectiveness of selected NOS controls for this client are separated into three categories: user account tests, group account tests, and password policy and system audit tests. Once you have answered all the questions in these categories, please draft a memo summarizing your findings. Attach detailed answers to all of the questions to your summary memo. A blank memo format is provided for you to use as an example (see Figure 3).

FIGURE 1
XYZ Organizational Chart

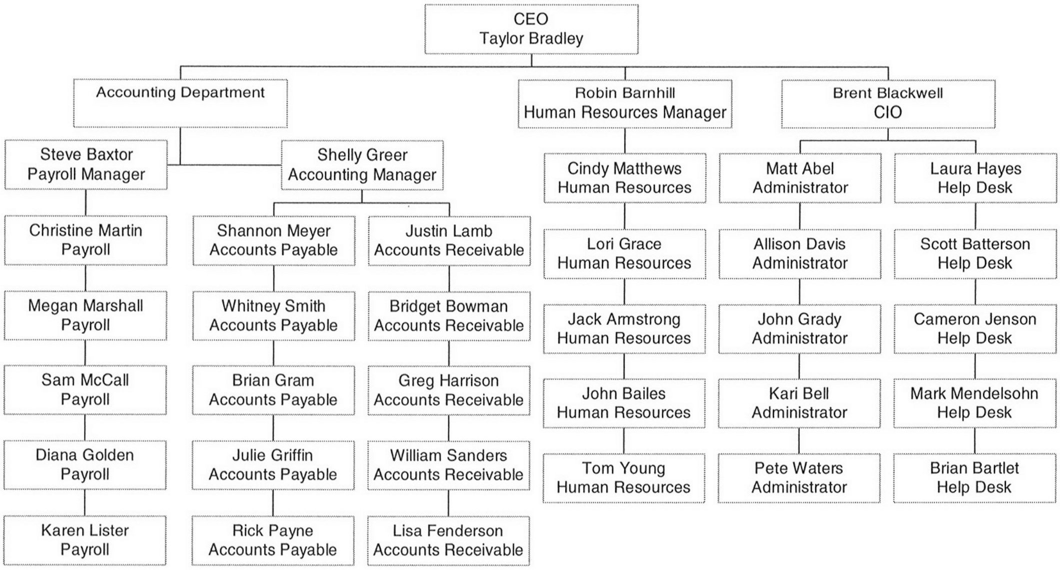


FIGURE 2
XYZ Password Policy

Password Policy for XYZ – 2002

In the interest of security, the following password policy has been drafted and approved by upper management. All staff must adhere to set policies. Failure to comply may result in disciplinary action ranging from a written reprimand to termination as determined appropriate by management.

- Minimum Password Age of 10 days
- Maximum Password Age of 60 days
- Minimum Password Length of 6 characters
- Password Uniqueness Required for 12 months
- Account Lockout set to Yes
- Account Lockout occurs after 3 bad logon attempts
- Account Lockout reset count in 1,440 minutes
- Lockout Duration set to forever

Passwords should not contain easily guessed words, such as words found in a dictionary. Passwords should be comprised of both upper and lower case letters, numbers, and special characters.

REQUIREMENTS

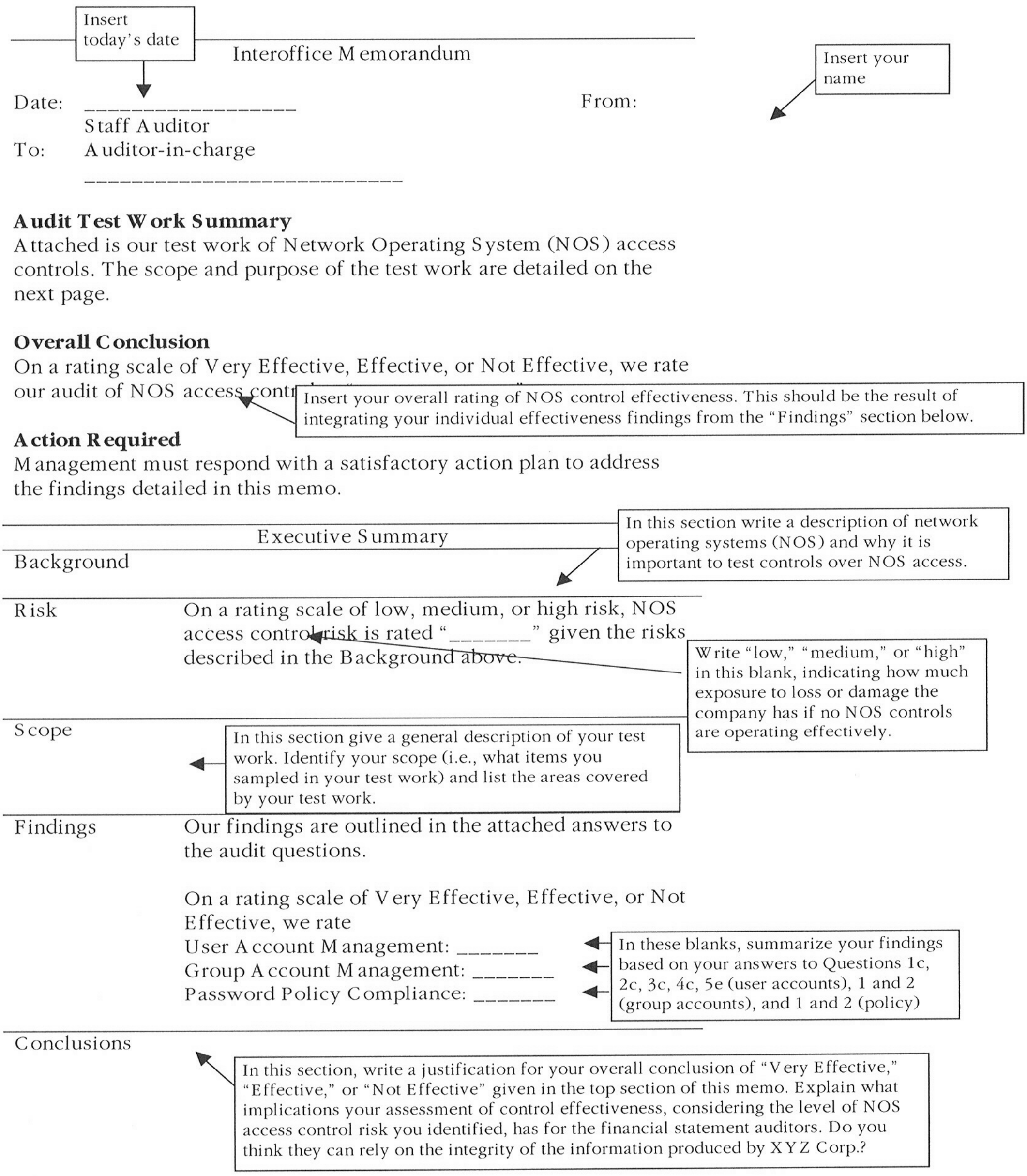
Part 1: User Account Tests

Necessary File: User Dump Text Data File

The user dump text data file contains details of the security settings for each user account. All fields in DumpSec's user data file are described for completeness purposes, but you will not use all of them when completing this assignment. The *UserName* field contains the user's logon name; sometimes this is called a screen name or a User ID. Each separate UserName represents a separate computer account that is assigned to a user. No two accounts can share the same UserName—the UserNames must be unique. You may notice that some UserNames in the casestudyusers.txt are repeated; that is because some of the user accounts belong to multiple user groups and a separate row in the file is needed for each group to which a user account belongs. The *Groups* field indicates a group to which a user account belongs. Each group represents a combination of system access permissions the system administrator has created commensurate with the expected need for different categories of employees. By creating groups, the system administrator avoids the need to set each separate setting individually for each user. Instead, the system administrator can set each separate setting for a group and then assign appropriate users to that group. Each user assigned to that group is automatically assigned the settings that were determined for that group. However, user account testing is important (rather than only testing group accounts) because settings assigned as a result of group membership may be overridden separately for each individual.

The *GroupComment* field contains a general description of the permission granted to the group and for many groups, and in many cases is left blank. The *GroupType* field indicates whether the group is global or local. The *FullName* field contains the first and last name of the user to whom the user account is assigned. You will notice that each repeated row for the same UserName also has the same FullName. The *AccountType* field specifies the type of account (e.g., user, group, etc.). The *Comment* field is available for any additional comment the system administrator wants to make for each account (if any). *HomeDrive* indicates which disk drive on the network is the drive on which the user's normal allocated disk space is located. *HomeDir* indicates which directory on the HomeDrive is designated as home for each user account.

FIGURE 3
Example Memorandum



Insert today's date

Interoffice Memorandum

Insert your name

Date: ___________________ From:

To: Staff Auditor
Auditor-in-charge
____

Audit Test Work Summary
Attached is our test work of Network Operating System (NOS) access controls. The scope and purpose of the test work are detailed on the next page.

Overall Conclusion
On a rating scale of Very Effective, Effective, or Not Effective, we rate our audit of NOS access contr

Insert your overall rating of NOS control effectiveness. This should be the result of integrating your individual effectiveness findings from the "Findings" section below.

Action Required
Management must respond with a satisfactory action plan to address the findings detailed in this memo.

Executive Summary

Background

In this section write a description of network operating systems (NOS) and why it is important to test controls over NOS access.

Risk

On a rating scale of low, medium, or high risk, NOS access control risk is rated "_______" given the risks described in the Background above.

Write "low," "medium," or "high" in this blank, indicating how much exposure to loss or damage the company has if no NOS controls are operating effectively.

Scope

In this section give a general description of your test work. Identify your scope (i.e., what items you sampled in your test work) and list the areas covered by your test work.

Findings

Our findings are outlined in the attached answers to the audit questions.

On a rating scale of Very Effective, Effective, or Not Effective, we rate
User Account Management: _______
Group Account Management: _______
Password Policy Compliance: _______

In these blanks, summarize your findings based on your answers to Questions 1c, 2c, 3c, 4c, 5e (user accounts), 1 and 2 (group accounts), and 1 and 2 (policy)

Conclusions

In this section, write a justification for your overall conclusion of "Very Effective," "Effective," or "Not Effective" given in the top section of this memo. Explain what implications your assessment of control effectiveness, considering the level of NOS access control risk you identified, has for the financial statement auditors. Do you think they can rely on the integrity of the information produced by XYZ Corp.?

A *Profile* is established by the Administrator (discussed below) and defines: (1) which functions from the desktop environment a user has access to (e.g., functions can be locked so that a user does not have access to Windows Explorer, Run, Command Prompt, or other functions on his or her tailored Start Menu), as well as (2) user's logon scripts and home directory location. A profile is a great control because it can be used to lock users out of sensitive system functions, such as the ability to install software or explore the network. Additionally, it can be used to disable CD-ROM and Floppy Drives so that users cannot introduce or remove data. The *LogonScript* field represents a script (or scripts) that is executed when a user logs on. The script can open application software and/or create environmental variables. The *Workstations* field is used to restrict particular workstations from which a user can log on. If this field is null (i.e., has no data value), then there are no workstation restrictions.

The *PswdCanBeChanged* field is assigned either a "yes" or "no" value to indicate the corresponding permission setting. If it is set to "yes," the user is allowed to change his or her password; if it is set to "no," the user is not allowed or able to change his or her password. *PswdLastSetTime* is a date/time field that indicates the date and time at which the password was last set. *PswdRequired* is a field that indicates whether each user account is required to have a password. If it is set to "yes," the user must enter a valid password to access his or her account; if it is set to "no," the user does not need to enter any password to access his or her account. *PswdExpires* is a field that indicates whether the password is set to expire. If it is set to "no," there is no limit to the useful life of a password. If it is set to "yes," the password will not allow access to the user account after a particular date. The *PswdExpiresTime* indicates the date and time after which the user will not be allowed to access his or her user account without having changed the password if the *PswdExpires* field is set to "yes."

The *AcctDisabled* and *AcctLockedOut* fields respectively indicate ("yes" or "no") whether each user account is currently disabled or locked out. The *AcctExpiresTime* indicates the date and time after which a user account will no longer be active and will not allow access to the system. The *TrueLastLogonTime* indicates the date and time of each user's most recent logon. *LastLogonServer* indicates the name of the server onto which each user most recently logged on. *LogonHours* indicates the hours that a user can log on to the system (if null, then a user can log on 24 hours per day). *SID* (security ID) is a unique number associated with a User ID (therefore, this is like a primary key in a relational database). Even if an account (e.g., jsmith) is deleted and recreated with the same username (jsmith), the SID will be different for the new account.

RAS is an acronym for remote access server. *RasDialin* allows for dialup (i.e., modem) access utilizing a Windows NT Server set up as a RAS server. This field can take on a data value of "yes" or "no." In this assignment RasDialin is set to "no," which suggests an aftermarket third-party RAS solution is being used. The *RasCallback* field is an outdated procedure for establishing a communication line via modem. With RasCallback: (1) users called in, (2) users were authenticated, (3) the communication line was broken, and (4) the RAS server called the user back at a predefined telephone number. RasCallback was an effective control since it typically precluded people from getting access via a "war dialer" (a tool that dials a bank of telephone numbers to see which allows remote access and then utilizes various combinations of user names and passwords to attempt to gain access). With the advent of a mobile workforce and laptops, this control is no longer effective and is rarely, if ever, used. RasCallback takes on a data value of "yes" or "no" to indicate whether the user is allowed to use RasCallback. *RasCallbackNumber* is the telephone number used for a specific user's RasCallback.

Purpose of User Account Tests

The purpose of testing user accounts is to determine if there exist any irregularities or weaknesses that could result in NOS vulnerabilities. For some testing, you need to determine appropriate membership in sensitive groups. On every NOS, there is a user or group of users that have ultimate access, i.e., access to everything in the system—these users are called "super users." In a Windows environment (such as the one used in this assignment), these "super users" belong to the Administrators and Domain Administrators groups. In a UNIX environment, these users are said to have "root" access. On an OS/400 system, these users are said to have "QSECOFR" access. Because of their unlimited access, it is crucial for firms to control the number of sensitive users.

From an audit and control perspective, it is crucial for organizations to control users who are "super users." Within a Windows environment, Administrators and Domain Administrators can create user accounts, create user groups, change ALL passwords for every user on the network, add/change/delete/view ALL files, install any type of software (even malicious code that captures User IDs and passwords when other users log on), modify security settings, modify audit settings, access files on OTHER computers within the network, and other tasks. In general, since Administrators and Domain Administrators are charged with maintaining the stability and functionality of the NOS, they have the ability to perform any task on the NOS. Given the unlimited rights that members in these two groups have, every effort should be made to ensure that proper controls exist over these two groups. Any weakness in controls over the Administrator and Domain Administrators groups represents a serious lapse in NOS controls. Auditors must identify which users have "super user" access and assess risk appropriately.

For your user account tests, you are required to evaluate controls over passwords, disabling of accounts, and stale accounts. A password represents the most common and weakest form of user authentication (identifying a valid user based on supplied credentials). Typical controls over passwords include: requiring a password, forcing periodic password changes by setting an expiration interval, and limiting the interval before a password may be reused. Accounts that do not require passwords represent an increased exposure because an unauthorized user needs only to guess a valid User ID. Given that many organizations subscribe to a first letter, last name User ID convention, the lack of a password requirement increases the likelihood of unauthorized access. Forcing users to change their passwords by having them expire after a specified time decreases the likelihood that an unauthorized user can gain long-term access with another's account. Allowing users to change their passwords on demand enables users to change their passwords in a timely manner in the event that they have been compromised.

A disabled account is one that has been manually "locked" by an Administrator or Domain Administrator. Accounts are typically disabled because the user is on extended vacation or leave of absence, or has been terminated. A "locked out" account is one that has been disabled for a specific time by the NOS due to excessive failed logon attempts (users trying to access the NS with a valid User ID but invalid password). A "stale" account is a user account that has not been accessed in a reasonable amount of time. Given that users need to access the NOS to use email, Internet browsers, and mission-critical business applications, an account that has not been accessed in 30 days or more represents a deviation from the business norm. In most instances, stale accounts are an indicator of a terminated employee or one on extended leave. Stale accounts represent opportunities for unauthorized users to gain access to the system, and since the accounts are not likely being monitored, their access is likely to go unnoticed for some time.

All NOS installations include default accounts and groups. In a Windows environment, the Administrator and Guest accounts are installed by default. Since it is common knowledge that every installation will have these accounts, special efforts should be taken to ensure that these accounts (and all default accounts) are properly controlled.

Required

(Note: For the purpose of this exercise, "sensitive users" and "sensitive user groups" are defined as users who have Administrator or Domain Administrator privileges and belong to the respective user groups.)

1. Password requirements:
    a. What risk exists if user accounts are not required to have passwords?
    b. List the user name of any accounts for XYZ that do not require passwords. How many users are on your list? What percentage of the total user population for this client does that number represent? Put an asterisk (*) next to any of these accounts that are members of sensitive groups (i.e., Administrators or Domain Administrators).
    c. Given your controls test in part 1 (b), rate the effectiveness of controls over password requirements as Very Effective, Effective, or Not Effective. Explain your rating.
    d. What would your control effectiveness rating have been if you had observed five normal user accounts for XYZ that were not required to have passwords? Explain your rating.
    e. What would your control effectiveness rating have been if you had observed one sensitive user account for XYZ that was not required to have a password? Explain your rating.
2. Password expiration:
    a. What risk exists if user accounts have passwords that never expire?
    b. List the user name of any accounts for XYZ that do not require passwords to expire. How many users are on your list? What percentage of the total user population for this client does that number represent? Put an asterisk (*) next to any of these accounts that are members of sensitive groups (i.e., Administrators or Domain Administrators).
    c. Given your controls test in part 2 (b), rate the effectiveness of controls over password expiration as Very Effective, Effective, or Not Effective. Explain your rating.
    d. What would your control effectiveness rating have been if you had observed three normal user accounts (and no sensitive user accounts) for XYZ that were allowed to have passwords that never expire? Explain your rating.
    e. What would your control effectiveness rating have been if you had observed one sensitive user account (and no normal user accounts) for XYZ that was allowed to have a password that never expires? Explain your rating.
3. Password changes:
    a. What risk exists if user accounts have passwords that can never be changed?
    b. List the user name of any accounts for XYZ with passwords that cannot be changed. How many users are on your list? What percentage of the total user population for this client does that number represent? Put an asterisk (*) next to any of these accounts that are members of sensitive groups (i.e., Administrators or Domain Administrators).
    c. Given your controls test in part 3 (b), rate effectiveness of controls over password changes as Very Effective, Effective, or Not Effective. Explain your rating.
    d. What would your control effectiveness rating have been if you had observed ten (nonsensitive) accounts for XYZ that had passwords that cannot be changed? Explain your rating.
4. Disabled/locked out accounts:
    a. Under what circumstances might a system administrator be well advised to disable an account or establish "lock out" settings?
    b. List the user name of any accounts for XYZ that have been disabled or locked out. How many users are on your list? What percentage of the total user population for this client does that number represent? Put an asterisk (*) next to any of these accounts that are members of sensitive groups (i.e., Administrators or Domain Administrators).
    c. Given your controls test in part 4 (b), rate the effectiveness of controls over password requirements as Very Effective, Effective, or Not Effective. Explain your rating.
    d. What if you observed the Administrator account was locked out? What if you observed no accounts were disabled or locked out? Explain your answer.
5. Note the date that the DumpSec report was run against the Primary Domain Controller:

a. What risk would exist if a user has never logged on to his or her account?
b. What risk would exist if a user has not logged on to his or her account in the last 30 days (but at some earlier time did log on)?
c. List the user name of any accounts for XYZ that have never logged on. How many users are on your list? What percentage of the total user population for this client is that number?
d. List the user name of any accounts for XYZ that have not logged on in the 30 days prior to the DumpSec report date (but at some earlier time did log on). How many users are on your list? What percentage of the total user population for this client does that number represent?
e. If we determine that the accounts identified in part 5 (c) are for brand new employees and the accounts identified in part 5 (d) are for employees who have been terminated, what should our recommendations be to the client XYZ? Why?

6. For each of the tests you performed for Questions 1 through 5 above, is the risk arising from each of the scenarios greater for sensitive group user accounts than for normal user accounts? Why or why not?

Part 2: Group Account Tests

Necessary File and Documentation: Group Dump Text Data File and Organizational Chart

The group dump text data file contains the details of group membership that determine which components of the information system the group is permitted to access. The *Group* field contains the name of the group. The *Comment* field contains a description of the capabilities of the group (it may be left blank). *GroupType* indicates whether the group is global or local. *GroupMember* contains the UserName of a member of the group. A separate row exists in the group dump text data file for each member of the same group. *MemberType* indicates what type of member the user account represents (e.g., User, Global, etc.).

The organizational chart is the standard against which the DumpSec group dump text data file is compared. That is, the organizational chart denotes the job responsibilities of each employee and thereby indicates what permissions the employee should have in the system. The group dump text data file shows what permissions each user account actually has been given in the system. An analysis of the organizational chart compared to the actual permissions provides insight into how well management controls system access within the organization.

Purpose of Group Account Tests

The group accounts must also be tested to determine whether any irregularities or weaknesses exist that could result in NOS vulnerabilities. In examining group accounts, auditors need to consider the job responsibilities of group members and determine whether their NOS access permissions are consistent with their job responsibilities. Such consideration includes segregation of duties and evidence that access permissions are not updated upon changes in job responsibilities. Only the information an employee needs to perform his or her job responsibilities should be accessible to that employee. In some cases access to excess information may not increase the risk of fraud. However, the company should have a valid reason for granting extended access. Allowing employees access to more data than they need to complete their job function unnecessarily increases the number of potential entry points for hackers. You are asked to perform the following group tests and include the results in your control assessment.

Required

1. For members in each of the following groups, compare their permissions in the DumpSec group report to their positions on the organization chart. Make a note of permissions that seem inconsistent with their job responsibilities. For each inconsistency, explain what area the group member has permission to access unnecessarily, and state whether there appears to be a risk *beyond* the increased number of potential entry points to the NOS.

a. Administrators (includes Domain Administrators)
b. Help Desk
c. Accounts Receivable
d. Accounts Payable
e. Payroll
f. Human Resources
g. Management

2. Assume that any discrepancies noted in Question 1 resulted from company personnel being transferred or promoted into new positions. Assume further that corporate policy says all system access changes due to termination or transfers must be enacted immediately upon transfer/termination. Given these assumptions, what is your assessment of the operating effectiveness of this policy as a system security control?

Part 3: Password and Audit Policy Tests

Necessary File and Documentation: Policy Extract Data File and Password Policy

The policy extract data file shows what policies have been implemented in the NOS. XYZ has a Corporate Password Policy developed to implement corporate standards with respect to password controls. A comparison of the Corporate Password Policy to the policy extract data file will reveal any discrepancies between management's objectives and the implementation of those objectives in the form of system enforced controls.

Logging system events and auditing these events represents an essential detective control. It is essential that system administrators establish sufficiently large log files to capture and retain events for a reasonable time to allow for review. Given the number of users and the vast volume of transactions that may be occurring on a network, using a small log file increases the likelihood that crucial system events that have been logged may be overwritten before a system administrator or IT security officer has the opportunity to review the logs for suspicious or inappropriate activity. The use of scripts (small "programs" that automate the execution of system commands) to continually execute "loggable" events combined with a small log file size represents a risk that critical events may be overwritten before they are reviewed. A program or application that crashes typically generates voluminous error messages and troubleshooting data in the logs, which for relatively small log files will result in the overwriting of valuable troubleshooting data.

Purpose of Password and Audit Policy Tests

A third category of NOS audit tests is the examination of password settings to determine whether they comply with the client's password policy, and the examination of policies and procedures surrounding the NOS audit function. The NOS audit function verifies network access activity against the permissions, and logs successes and/or failures depending on specified audit policies. These activities are recorded in a file called a security audit log. Companies specify a maximum size for the audit log file. Once the audit log is filled, the company can choose to have the system shut down (crash) or continue processing without keeping additional records of exceptions. You are asked to perform the following password and audit policy tests and include the results in your control assessment.

Required

1. Inspect the Account Policies Password Settings. Do the password settings comply with the corporate password policy as set forth in the document provided by the client? If not, explain what discrepancies you identified.
2. Inspect the audit policy and note the setting for "CrashOnAuditFail." If this setting is "true," it means the NOS will deny all additional accesses once the audit log is full. If it is "false," the NOS will continue to allow accesses once the audit log is full. Given the current setting for this field, what risk is there (if any) to XYZ Corp? What damage might a hacker be able to inflict (if any)?

LEARNING OBJECTIVES AND IMPLEMENTATION GUIDANCE

Introduction

In this section we describe the intended audience for this assignment, the learning objectives and use of materials, and student feedback. Instructors may choose to implement this assignment using either Microsoft™ Excel PivotTables or Microsoft Access queries. The goal of this assignment is not to teach the technology itself, but to provide an experiential learning situation in which students can use the technology as a tool to help identify substantive risks associated with NOS security. Therefore, the emphasis should be placed on the risks and the related controls. Student feedback revealed that students believed this assignment was a valuable learning exercise worth their time and effort.

Intended Audience

This assignment is appropriate for use by undergraduate or graduate students in an accounting information systems, audit, or systems audit course. The most appropriate course in which to include this assignment depends on the specific university curriculum, especially because some universities require accounting information systems as a prerequisite for auditing, and vice versa. Students should have basic prerequisite knowledge in the areas of computer controls, general internal controls, and network operating systems commonly found in accounting information systems textbooks. (For example, see Hollander et al. 2000; Romney and Steinbart 2003; Gelinas and Sutton 2002.) We have used this assignment in accounting information systems classes; students complete the assignment after we have covered risks and controls. These students had not yet taken an audit course, as AIS is a prerequisite to an audit course in their curriculum.

Learning Objectives and Use of Materials

The purpose of this assignment is to provide students with a realistic context in which to learn about network operating system controls and to evaluate compliance with those controls. The assignment also provides students with a skill-building opportunity, using one or more technology tools to help them conduct audit assessments. The assignment includes an overview detailing the nature of the audit work to be performed and a related list of questions to be answered. Supporting materials include a series of three file dumps, an organization chart, a corporate policy describing password usage, and an optional database shell. Although Windows NT™ is used as the simulated NOS environment in this assignment, the concepts included in the assignment are generalizable to other NOSs (such as UNIX and OS/2). To adapt this assignment to another NOS would require considerable effort, as an instructor would need to identify an appropriate utility program similar to DumpSec for the desired NOS, and prepare alternative data files that contain the data fields that would be produced by that utility. Appropriate terminology revisions would also need to be made in the assignment. Although the data files produced by utilities similar to DumpSec for alternative NOSs are different, the information contained in them is similar, as are the recommended audit tests. In using this assignment with any NOS, it is important for instructors to stress concepts over the specific NOS choice.

The materials (i.e., the assignment, three text files, organization chart, corporate password policy, and database shell) should be distributed to students in their entirety. Instructors may download these materials from the *Issues in Accounting Education* Teaching Notes website and post them on their own course websites or make them available to students on a diskette. Instructors may want to change the dates as the data files become older to make them more current. The database shell has all of the queries needed for this assignment—the students merely need to import the text files into the Access database shell and then run the queries. Appendix A provides supplemental instructions for importing text file data into a Microsoft Access database (for instructors choosing to use the database shell). This is the approach practitioners usually take (i.e., they develop a database shell and then use it on all similar audits). Instructors wanting students to gain firsthand experience developing queries could require students to develop the necessary queries, and the database shell could be a suggested solution (in which case the instructor should not distribute the database shell to students). A final alternative, for instructors who prefer not to use Access, is to require students to import the text files into Excel and create PivotTables (which allow very simple querying). Appendix B provides supplemental instructions for importing text file data into Microsoft Excel and creating PivotTables. One major advantage of database queries over PivotTables is the reusability of queries. However, given the low volume of data in this assignment, PivotTables are a reasonable alternative.

The introduction and overview in this assignment are intended to expose students to how practitioners perform tasks like those in this assignment, and to provide definitions of the technical terminology used. To be completely realistic, students would need to be given access to a full NOS and to all user profiles such that they could replicate tasks performed by the security specialists. Unfortunately, such comprehensive access to a NOS is impractical in most academic settings. Therefore, this assignment abstracts from the ideal setting by providing text files from a fictitious company's NOS.

Student Feedback

In two undergraduate AIS courses at two universities, we class tested the Excel pivot table and database query creation alternatives over the course of several semesters. Student feedback from each administration was favorable, and we made changes to the assignment based on feedback from students, two anonymous reviewers, and the associate editor, Tom Hall. For purposes of illustrating assignment efficacy we report only the most recently collected data (which is consistent with data we collected with earlier versions of the assignment). The data presented here are based on an assignment in which students used Excel PivotTables for some of the audit tests and developed queries in Access for others. Although this hybrid approach was reasonably successful, we do not, in retrospect, recommend it because we believe the assignment should focus on only one tool (either Access or Excel) to help emphasize the risk and control concepts relative to the technology. Students who created Access queries found that requirement to be frustrating, even with the provision of screen shots to assist them in developing the queries. To reduce frustration and increase realism, we recommend use of the database shell option. Forty students completed the pre-assignment survey (pretest), the assignment, and the post-assignment survey (posttest) reported on herein. For both surveys students responded to a series of questions using seven-point rating scales.

Several precautions were taken to obtain reasonably reliable data. The overall topic of NOS controls was covered briefly in a textbook chapter and in more detail by a guest speaker, and was included on a unit examination prior to the assignment administration. Thus, any differences between the pre-assignment and post-assignment survey responses should be due solely to the assignment. A demand effect influencing student responses cannot be ruled out. However, precautions were taken to minimize any demand effect as follows.

The pre-assignment survey was administered two days before the assignment was distributed and a week before it was due. Students were told the instructor wanted feedback regarding their knowledge and comfort level as to some course-relevant materials. Students were encouraged to be honest and forthright in their responses. They were assured that their responses would not affect their grades; each questionnaire was identified by codes instead of names. Students were asked to write their name next to the corresponding code on a master list. However, they were informed that the names would be used only by a graduate assistant (not the instructor) to award extra credit to those who turned in completed surveys. They were assured that the master list would then be shredded and the questionnaire data would be compiled without names. The post-assignment survey was administered on the day the assignment was collected and similar procedures were implemented to encourage students to be honest and forthright in their responses. Students who completed both the pre-assignment and post-assignment surveys were awarded six extra credit points—less than 1 percent of the course grade.

The pre- and post-assignment data were intended to gauge students' previous knowledge and comfort level with the topics covered in the assignment, and compare these to their post-assignment knowledge and comfort level. Student responses using paired sample t-tests on the mean difference score (posttest minus pretest) are summarized in Table 1. A comparison of pre-assignment responses to post-assignment responses reveals a significant increase in student perceptions in the following areas:

- knowledge of general internal controls
- knowledge of system security controls
- knowledge of network operating systems (NOS)
- knowledge of password protection issues
- comfort with assessing risk associated with NOS controls
- comfort importing text files into Excel
- comfort using PivotTables in Excel
- comfort importing text files into Access

The first five topic areas in this list encompass the main objectives of the assignment; therefore we expected this significant increase in students' knowledge and comfort level even though these issues had been discussed in class sessions. The last three topic areas on this list represent technical skills that had not been covered in the course in any format prior to the assignment. For most students in the course, the assignment instructions were the only coverage of these skills in the school's curriculum. Therefore, we expected increases in knowledge and comfort levels for these topics.

An unexpected result was that students felt less comfortable using Access tables and no more comfortable creating queries in Access after completing the assignment. Students had created and used Access tables in an extensive project prior to completing the assignment, but they had not created queries prior to this assignment. It is possible that before completing the assignment, the students were overconfident of their Access abilities. Open-ended feedback obtained after the assignment was completed revealed that students had difficulty importing the ASCII text file data into database tables and also had difficulty formulating queries in Access. The instructions given to students were purely textual, with very few screen shots and no annotations. The two previous administrations of the assignment had only employed Excel PivotTables. Because frustration with software is obviously not a desired objective of this assignment, we developed the database shell and improved the instructions for importing the text file (Appendix A).

Finally, for the remaining survey responses no statistically significant differences were noted:

- belief in importance in evaluating NOS security during financial audit
- belief that auditors need to know how to evaluate NOS controls

The nonsignificant differences in the importance of evaluating NOS security during a financial audit and the belief that auditors need to know how to evaluate NOS controls were unexpected. However, the mean values on these questions were relatively extreme on the pre-assignment survey: (the mean response to "I believe it is important to evaluate network operating system security when assessing risk for a financial statement audit" was 5.9 and the mean response to "I do not think financial statement auditors need to know how to evaluate network operating system security controls" was 2.1); so perhaps they could not reasonably be expected to increase. In other words, students were apparently convinced of the importance and of the need to know how to evaluate NOS security and controls before they completed the assignment. Completion of the assignment did not serve to change their minds, it merely confirmed their conviction.

TABLE 1
Comparison of Pretest and Posttest Questions Using Paired Sample t-tests

Question	Difference Score Mean[a] (Standard Deviation)	t -value
1. Rate your level of knowledge of general internal controls.	0.5 (0.9)	3.4***
2. Rate your level of knowledge of system security controls.	0.5 (1.3)	2.6**
3. Rate your level of knowledge of network operating systems.	0.6 (1.4)	2.7**
4. Rate your level of knowledge of password protection issues.	0.4 (1.1)	2.5**
5. Rate how comfortable you feel assessing risk associated with network operating system controls.	0.7 (1.4)	3.0**
6. Rate how comfortable you feel importing data from ASCII (text) files into Microsoft™ Excel.	2.3 (2.4)	6.1***
7. Rate how comfortable you feel using PivotTables in Microsoft Excel.	2.0 (2.3)	5.4***
8. Rate how comfortable you feel importing data from ASCII (text) files into Microsoft Access.	2.4 (2.3)	6.5***
9. Rate how comfortable you feel using Microsoft Access tables.	–0.5 (1.6)	–2.0*
10. Rate how comfortable you feel creating queries in Microsoft Access.	–0.1 (1.8)	–0.5
11. I believe it is important to evaluate network operating system security when assessing risk for a financial statement audit.	0.3 (2.2)	0.8
12. I do not think financial statement auditors need to know how to evaluate network operating system security controls.	–0.5 (1.8)	–1.6

Responses are based on a series of seven-point scales with 7 labeled "high knowledge," "highly comfortable," and "strongly agree" (for questions 1–4, 5–10, and 11–12, respectively), and 1 labeled "low knowledge," "highly uncomfortable," and "strongly disagree," respectively. Difference score is calculated by posttest rating minus pretest rating. Significance testing is based on one-tailed t-test. Numbers are rounded to nearest tenth.

*, **, *** $p < .05$, $p < .01$, and $p < .001$, respectively.

[a] n = 40.

SUMMARY

Overall, students appeared to enjoy the assignment, and believed they learned from the resource and that completion of the assignment was worth their time and effort. According to experiential learning theory (Rogers 1969; Rogers and Freiberg 1994), learning is facilitated when students participate in the learning process and when they are directly confronted with practical, social, personal, or research problems. This assignment confronts students with a realistic practical problem and requires them to participate in the learning process; thus it facilitates learning. Evaluation of NOS controls is a valuable skill in practice that requires consideration of materials similar to those included in this assignment. Students who develop skills for evaluating these controls in an academic setting will be well prepared when they enter the professional world.

TEACHING NOTES

Teaching Notes are available through the American Accounting Association's new electronic publications system at http://aaahq.org/ic/browse.htm. Full members can use their personalized usernames and passwords for entry into the system where the Teaching Notes can be reviewed and printed.

If you are a full member of AAA and have any trouble accessing this material please contact the AAA headquarters office at office@aaahq.org or (941) 921-7747.

REFERENCES

Auditing Standards Board. 2001. *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit.* Statement on Auditing Standards No. 94. New York, NY: AICPA.

Gelinas, U. J., and S. G. Sutton. 2002. *Accounting Information Systems.* Fifth edition. Cincinnati, OH: South-Western Publishing.

Hollander, A. S., E. L. Denna, and J. O. Cherrington. 2000. *Accounting, Information Technology, and Business Solutions.* Second edition. Burr Ridge, IL: Irwin/McGraw-Hill.

McClure, S., J. Scambray, and G. Kurtz. 2001. *Hacking Exposed: Network Security Secrets and Solutions.* Third edition. Berkley, CA: Osborne/McGraw-Hill.

Rogers, C. R. 1969. *Freedom to Learn.* Columbus, OH: Merrill.

———, and H. J. Freiberg. 1994. *Freedom to Learn.* Third edition. Columbus, OH: Merrill/Macmillan.

Romney, M. B., and P. J. Steinbart. 2003. *Accounting Information Systems.* Ninth edition. Upper Saddle, NJ: Prentice Hall.

SomarSoft. 2001. SomarSoft utilities. September 30. Available at: http://www.somarsoft.com/.