AN EXPERT SYSTEM FOR AUDITING DATA COMMUNICATIONS

By

PATRICK DEAN FETT

Bachelor of Science
in Business Administration
The Ohio State University
Columbus, Ohio
1982

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
July, 1989

AN EXPERT SYSTEM FOR AUDITING

DATA COMMUNICATIONS

Thesis Approved:

Thesis Adviser

G. E. Hedrick

M. Samadzadeh

Norman N. Durham
Dean of the Graduate College

PREFACE

An expert system for auditing data communications was developed. This system assists an auditor in performing an Electronic Data Processing (EDP) audit of a data communication network. The expert system has several features specific to the auditing profession. These features include documentation of work performed, presentation of preliminary findings, drafting the audit report, and determination of the audit opinion. A copy of the expert system developed for this study is available through the Computing and Information Science Department of Oklahoma State University.

I would like to express my gratitude to my advisors Dr. K. M. George, Dr. G. E. Headrick, and Dr. M. H. Samadzadeh for their support and guidance during my thesis.

I would also like to thank my employer, E. I. du Pont de Nemours and Company, who both encouraged me to attend graduate school and provided financial support. Especially Ken Baker, who supported my studies and arranged my travel schedule so I would be able to attend classes.

Thanks also to Dawn Ann Mendenhall for her expert proofreading of this thesis.

Finally, many hugs and kisses to my wife, Lorraine, and my daughter, Leah. Their patience and loving support made this endeavor possible.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Computers in the Audit Function

Today, computers are being widely used by the audit profession. Historically, much of a company's computer data was stored on mainframe computers and minicomputers. Access to the computer was generally limited to obtaining reports that would assist the auditor in the manual process of performing an audit. The programs that created these reports were usually developed by a specialized group of Electronic Data Processing (EDP) auditors.

The development of the personal computer has accelerated the process of computerization for the audit profession. The laptop computer was an especially important development because it allowed auditors to take computing on the road. The auditor can now use the personal computer to perform data analysis, document work, draft audit reports, and communicate their findings to management.

To date, most audit applications have involved the use of electronic spreadsheets, word processors, and data base applications. In addition, computers are being used for audit scheduling and electronic communication known as E-mail.

A relatively new field is the development of audit expert systems. These systems will automate the audit process by analyzing audit data and generating recommendations. These systems have many potential benefits cited in the literature. Chapter II will address the benefits in detail. A summary of the benefits follows:

- Reduced cost
- Faster audits
- Higher quality audits
- More consistent quality
- New auditor training
- Providing time for new services
- Preservation of expertise

Intent of Study

The intent of this study is to determine the features needed in an expert system that will be used by internal auditors and to implement these features by developing an expert system for auditing data communications networks.

The features needed in an audit expert system were determined by a review of literature and the author's own experience as an EDP auditor. These features are described in detail in Chapter II and are listed below in summary. They are the following:

- Collect and evaluate audit evidence
- Document user input
- Process uncertain user input

- Explain why conclusions are drawn in a way that will train new auditors
- Identify audit exceptions and determine which should go in the final report
- Determine the audit opinion

These features were implemented in an expert system that will assist an EDP auditor in performing an audit of a data communications network.

CHAPTER II

REVIEW OF LITERATURE

Introduction

This section provides background information related to this thesis. It identifies the current method of performing audits, current audit expert system prototypes, and features needed in an audit expert system. It is composed of the following sections:

- Domain Information
- Benefits of an Audit Expert System
- Appropriateness of Audit Domain
- Review of Current Audit Expert System Prototypes
- Features Needed in an Audit Expert System

Domain Information

Auditing Function Description

The function of internal audit is to be the eyes and ears of corporate management. It is internal audit's task to review all aspects of a company's business for compliance with company policies and procedures. Internal audit reviews all company operations to determine whether the system of internal control is adequate and functioning in a way that protects the assets of the company.

Data is one of the assets of the company. Thus, all data processing areas are subject to review by audit to determine whether controls are adequate to protect data from unauthorized disclosure, modification, or loss. The data communications network is one of the data processing areas reviewed by EDP auditors.

Audit Methodology

The present audit methodology described in the following paragraphs is used by the author at E. I. du Pont de Nemours and Company. Other organizations would use a similar methodology; however, there may be some differences. Any expert system that replaces the present methodology must provide similar capabilities.

Audits are performed by following the steps of an "audit program", which is a checklist of questions and test procedures. The purpose of the audit program is to ensure completeness and consistency between audits of the same subject. Audit programs contain some of the knowledge used by auditors, but do not document the advanced judgments of experienced or expert auditors. The audit program that was used as the basis for the development of this study can be found in Appendix A.

All work completed while following the audit program is documented in "audit workpapers". They document the responses to questions and the results of testing. Workpapers are kept for future use. They are helpful to the auditor preparing for the audit the next time it is scheduled.

Potential problems identified during an audit are reported to line management with auditing's recommendation for corrective action. These potential problems are documented in a preliminary audit report (PAR). The PAR is also kept in the workpapers. The significant PARs will be documented in a formal report to line management and their supervision.

Additionally, an audit opinion is furnished to management on the adequacy of controls in the area reviewed. The opinions given are strong, adequate, or weak.

Benefits of an Audit Expert System

A review of literature cites many potential benefits of using expert systems in auditing. These benefits include reduced cost, faster audits, higher quality audits, more consistent quality, new auditor training, providing time for new services, and preservation of expertise.

Audit costs should be reduced since audits can be performed faster. Also, the expert system could help train new auditors reducing training cost and the amount of supervision needed during an audit [2, 5, 6, 11].

Audits may be performed faster because the expert system would prompt the auditor with only necessary tasks.

This would keep them from being sidetracked. Also, audit time would be reduced because the system would make many of the time-consuming decisions for the auditor [11].

Audit quality may be improved when an expert system is used because judgments are being made based on an expert's knowledge. Also, an expert system should eliminate the possibility that audit steps might be skipped accidentally [2, 4, 11].

Audit quality may be more nearly consistent because all auditors are using the same procedures and knowledge base and personal auditor bias should have less effect on the outcome of an expert system [3, 6, 11].

Expert systems should provide a simpler way to train new auditors. Help screens within the expert system should explain to the new auditor what they are doing and why it needs to be done. This will greatly reduce the amount of direct supervision needed for new auditors and could reduce the associated training costs [3, 11].

Due to the time savings anticipated above, there should be more time for providing new services to clients. Instead of spending a large amount of time "pushing papers", the auditor can perform more analytical services for their clients [4, 11].

When experienced auditors transfer or leave the company, a large amount of auditing expertise can be lost. Expert systems can be a method of retaining this knowledge so other auditors can use it and learn from it [3].

Appropriateness of Audit Domain

Hayes-Roth, Waterman, and Lenat [9] give two important criteria for choosing domains for expert systems. They say you should choose a specialty area that does not rely on a lot of common sense, and the task should not be too easy or too difficult for a human expert to perform.

An expert system which is limited in scope to a particular audit subject should be a sufficiently narrow specialty. The expert system to audit data communications networks fits the first criteria. The proposed system also meets the second criteria. Instead of relying on common sense, there are specific internal controls that are reviewed in each subject area.

Much of the information used by auditors in assessing internal controls can be either qualified or quantified, so it can be entered in an expert system. Other decision support systems, like modeling, are not able to process the large amount of qualitative data involved in audit judgments, so expert systems are the best application choice [3, 8].

Another criteria considered to be essential for expert systems is that there are people within the domain that are considered to be experts and that they perform better than novices [5]. This criteria is also met by the audit function. Considerable training is needed to be an expert auditor. Also, expert auditors are better performers than novice auditors [3].

Another aspect of auditing is that it is an iterative process. The information learned at one point suggests further questions that need to be asked related to that information. This corresponds to the way expert systems ask only relevant questions based on answers to previous questions [2].

Review of Current Audit Expert System Prototypes

Several prototype systems have been developed to audit specific subject areas. No general auditing expert system has been developed. These expert systems are described below to give an overview of existing systems. All of them were reviewed by Chu [3] and Connell [5].

EDP-EXPERT provides a general review of all EDP internal controls. Its primary purpose is for use by external auditors when they are determining if they can rely on computer internal control systems.

AUDITOR is used by external auditors to determine if the allowance for bad debt is reasonable. Thus, the knowledge domain of this system is very narrow scope.

ICES is used to review internal controls in the area of accounts receivable transactions. The system provides assistance for less experienced auditors.

CFILE is an expert system used to evaluate banks, specifically their reserve for bad loans. The system is designed for senior auditors.

CHECKGAAP is used by experienced external auditors to verify compliance with the United Kingdom Companies Act.

The primary similarity of these systems is that they are developed generally for external auditors, but do not cover internal controls in the detail that internal auditors would. Also, most of these systems are targeted for the experienced user instead of the new auditor.

Features Needed in an Audit Expert System

There are several features that would be necessary in an audit expert system. Some of these features would be unique to the auditing profession. These features were determined based on related literature and the author's personal experience as an EDP auditor. The features that are implemented in the expert system developed for this study are the following:

Collect and Evaluate Audit Evidence

This is a basic feature of the audit process. Data is collected and evaluated by the auditor. The expert system must be able to prompt the user to enter the data needed for making conclusions [2].

Document User Input

Workpapers are a current necessity of the audit process. This is also true for an expert system. All auditor answers and expert system conclusions must be documented [2].

Process Uncertain User Input

The expert system must be flexible. Expert auditor's judgment is sometimes fuzzy. They are not always 100 percent sure of their facts or conclusions [1].

When people are asked to give an indication of how certain they are about some situation, the results can vary widely. The best way to reduce this effect is to separate the uncertain data into as many sub-components as possible. Some of these may be objectively answered reducing the overall uncertainty of the problem [10].

Explain Why Conclusions Are Drawn in a Way That Will Train New Auditors

Using the expert as a training tool for new auditors is one of the desired benefits of the system. Standard explanation facilities normally tell why a question is being asked based on a line of reasoning approach. A new auditor needs to know more including background information on the question [10].

Identify Audit Exceptions and Determine Which Should Go in the Final Report

When the expert system reaches the conclusion that there is a potential exposure, it must document this in a preliminary audit report (PAR). The PAR should document the problem, potential exposure, and the recommended solution [2].

Determine the Audit Opinion

An overall opinion is also determined for each audit. This opinion can be used by management to determine the state of the internal controls within the area audited. There are three opinions: strong, adequate, and weak [2].

CHAPTER III

PROJECT LIFE CYCLE

System Concept and Feasibility

There are several factors that explain why this project was chosen for study.

First, expert systems are still very new in the field of auditing. The complexity of auditing has slowed their development. Most of the existing prototype systems do not address internal controls at a depth sufficient for internal audit.

Second, audit work has several special needs unique to the profession. These features are documented in the last section of Chapter II. Their implementation is described in the Software Design and Coding section of this chapter. Some of these features, such as providing a high level of explanation and determining an audit opinion, are a significant step forward from current systems.

Third, based on the expected benefits of expert systems to auditing, there are significant benefits to be obtained from developing a usable expert system.

Finally, this project is closely related to the author's profession as an EDP auditor. The expert system that has been developed should be helpful in performing data communications audits.

The feasibility of an audit expert system has already been shown in the literature review in Chapter II. There have been several prototype systems developed that have obtained some level of success. The system developed for this study provides additional features to make it more useful to an auditor.

User Requirements Gathering and Analysis

The review of literature relating to audit expert systems suggested several requirements for an audit expert system. In addition, the present audit methodology suggests the need for additional requirements. The requirements that were implemented in this study are the following:

- <u>Collect and Evaluate Audit Evidence</u> - The expert system must be able to prompt the user to enter the data needed for making conclusions and then evaluate that data to reach conclusions.
- <u>Document User Input</u> - The expert system must be able to document the work performed during the audit. This takes the form of workpapers which are a current necessity of the audit process. All auditor answers and expert system conclusions must be documented.
- <u>Process Uncertain User Input</u> - The expert system must allow the auditor to express their certainty in facts that may not be clearly true or false.

- <u>Explain Why Conclusions Are Drawn in a Way That Will Train New Auditors</u> - The expert system must be able to be used as a training tool for new auditors. Also, the explanation facility should be able to tell why a question is being asked. This explanation would describe the internal control risk associated with each choice.
- <u>Identify Audit Exceptions and Determine Which Should Go in the Final Report</u> - The expert system must be able to determine potential exposures and document them in a preliminary audit report (PAR). The PAR should document the problem, potential exposure, and the recommended solution.
- <u>Determine the Audit Opinion</u> - The expert system must be able to determine an overall opinion of the state of internal controls within the area being audited. The three opinions that it must decide between are: strong, adequate, and weak.

Software Design and Coding

<u>Expert System Shell</u>

The expert system was developed using the Insight 2 + expert system shell, which uses a production rule language. A rule is the basic unit of the knowledge base. It contains information about what conclusions can be drawn based on particular facts. Facts are information supplied by the user of the system and the knowledge base developer.

Insight 2 + allows for object facts (has a characteristic associated with it), simple facts (true or false), numeric facts (integer or reals), and string facts (text value). The format of a rule is shown in Figure 1.

```
RULE 115 is there manual control of dial access
IF   dial access is available on the network
AND  the operator manually controls dial access
THEN manual control of dial access reviewed
AND  FILE manual control document
ELSE manual control of dial access reviewed
AND  FILE no manual control document
```

Figure 1. Example of a Production Rule

The above rule shows some of the complexity and flexibility of the system. The RULE keyword identifies this as a rule statement and gives it a name that can be used with the debugging/tracing tools provided by Insight 2 +. The next two lines (IF/AND) give the condition being evaluated by the rule. The next two lines (THEN/AND) give the conclusion and action to be taken if the condition is true. The last two lines (ELSE/AND) give the conclusion and action to be taken if the condition is false.

Insight 2 + Facilities

Some of the major features of the Insight 2 + expert system shell are the following:

- Facts and conclusions can be initialized at the start of the program. This is a very useful feature during testing. It allows specific tests to be completed without requiring the developer to repeatedly respond to all preliminary questions.

- An interface is furnished to access DBASE III data base files. This could allow the knowledge base to make use of existing data base files.
- The testing/debugging facilities allow you to trace the steps that the expert system followed in reaching its present point within the knowledge base.
- It is possible to call other executable modules from the expert system. These could provide further functions that are not supplied by the expert system shell.
- It is possible to "jump" to another expert system. This is done through the CHAIN command. This can be used to divide knowledge into logical subdivisions. It also can increase the maximum size of an application.

Development Methodology

Expert system development lends itself to an iterative development methodology. The first pass at developing the expert system was to write the first rule which subdivided the problem into the major areas that must be reviewed to complete the audit. A second iteration developed rules to cover what must be accomplished for each of these major areas to be reviewed. On further iterations, these subareas are further broken down to one or more questions that allow specific policies and procedures to be reviewed.

General Features of the Application

The knowledge base for this application consists of seven modules with a total of 83 rules and 401 facts. The expert system was designed and developed as seven knowledge base modules that are linked using the Insight 2 + CHAIN command.

Splitting the expert system into seven knowledge bases modularized the system along subsections of the audit program. It also allowed development and testing to be completed in a phased approach and shielded each module from changes made to any other module.

The audit application that has been developed differs from many expert systems. Its goal is to review all areas applicable to a data communications audit. When it finds a potential problem with security or integrity of the network, it notes the problem and continues its search for other problem areas. Many expert systems are designed to find the first problem and then stop. To have the system search for all problems, the goal had to be written as "controls reviewed" instead of "find a potential audit exception".

The following sections describe how each of the features of the expert system were designed and developed.

Collect and Evaluate Audit Evidence

This feature of the expert system is, of course, the backbone of the system. The other features enhance the system's basic usefulness, but collection and evaluation of audit evidence are the heart of the system.

The design of the expert system was based primarily on an audit program for reviewing data communications networks. This provided a general set of questions that are asked during a data communications audit. This audit program can be found as Appendix A.

Additional questions were developed based on the author's experience in performing data communications audits. The author's experience was especially helpful in developing the explanations for why each question was being asked.

Document User Input

This feature is accomplished by use of the Insight 2 + FILE command. Figure 1 shows an example production rule where the FILE statement causes the text described as "manual control document" to be written to an ASCII file. The "manual control document" text is described later in the program by use of the DISPLAY statement such as the one shown in Figure 2 on the next page. Variable information can be included in the DISPLAY statement to document numeric or character string facts entered by the user.

Each of the seven modules in which the knowledge base has been separated has its own log file where the expert system writes its documentation. There can be only one open file at a time so it is necessary to write both the workpapers and the audit report to the log file at the same time.

```
DISPLAY dial access protection par A
     C.      Manual activation/deactivation of lines
             is not used to protect dial in lines

             See item B above
```

Figure 2. Example DISPLAY Statement

A basic program was written to combine the log files from the seven modules and then separate the workpapers and audit report into two files. This program is listed in Appendix B - Log Program Listing. The workpapers resulting from the system test are listed in Appendix C - Workpapers Test Results. The audit reports resulting from the system test are listed in Appendix D - Audit Report Test Results.

Typically, workpapers are saved until the next time an audit is performed at the site. These help the next auditor prepare for the assignment. This can also be done with the expert system. The expert system and the user responses to questions can be saved to disk. This can be reloaded at another time. The user can review the previous responses and change the responses that are different.

Process Uncertain User Input

Some of the data processed by the expert system is judgmental. For example, the question, "Are data sets adequately protected?" requires the auditor performing the audit to make a judgment. This type of question may be difficult to answer either yes or no, and the auditor may not be certain of their answer.

There are several examples of this type of question in the knowledge base. Uncertainty is handled by using the confidence level facility provided by the expert system shell. Instead of answering true or false to this type of question, the user is prompted to adjust a confidence bar from zero to 100 by using the left and right cursor keys. Figure 3 shows an example CONFIDENCE statement which causes the associated facts to be queried with the confidence bar instead of true and false.

```
CONFIDENCE but access policy not needed
AND        Dial access protection F
AND        updates and access to control and routing tables
           is adequate
```

Figure 3. Example Confidence Statement

The expert system can process the confidence bar response in several ways. A threshold value can be set that determines whether the fact is considered true or false.

Normally, the threshold is set at 50, but this can be set for each question. Another method of processing the confidence level is to use the Insight 2 + CONF function, which will return a numeric value from zero to 100 representing the confidence level. This function can be used in a conditional statement of the production rule language.

Explain Why Conclusions Are Drawn in a Way That Will Train New Auditors

Standard expert system shell explanation function tells the user why a question was asked based on the current line of reasoning. The expert system that has been developed for this study uses the Insight 2 + EXPAND feature to provide additional assistance to the user regarding why a question is asked.

Figure 4 on the next page shows an example EXPAND statement. This statement repeats the original question, provides additional background information, explains what exposure is being reviewed, and explains what the auditor should look for before answering the question. The type of information provided to the user should improve the quality of their answers and provide training to auditors unfamiliar with data communications audits.

```
EXPAND outgoing ports protected

     Review security for outgoing ports and modems of the
     callback system.  If someone can dial into the outgoing
     port, they may be able to gain unauthorized access to
     the system unless the phone system or modem stops them.
     Is there some method to block attempts to gain access
     through the outgoing ports?  If so, answer TRUE.
     Otherwise, answer FALSE.

     Test of callback systems show that some are vulnerable
     to a hacker calling an outgoing port.  The callback
     system will not answer the hacker, but the next time
     the callback system uses that outgoing port to try to
     connect to a legitimate user, it will answer the call
     without knowing.  If the hacker plays a recording of a
     dial tone, the callback system will assume it got an
     outgoing line and dial the number.  The hacker can then
     simulate answering the phone and send the computer tone
     to connect to the network.

     Some systems get around this by requiring the caller to
     reverify their identity.  Also, many phone systems can
     configure a phone number for outgoing calls only.  The
     caller then gets a busy signal or a message that the
     number is invalid.
```

Figure 4. Example EXPAND Statement

Identify Audit Exceptions and Determine Which Should Go in the Final Report

Audit exceptions are determined based on the user responses to questions in the knowledge base. When the expert system determines there is an audit exception, it is displayed on the screen. Exceptions that are to be included in the audit report are also written to the log file. Figure 5 on the next page shows an example DISPLAY statement for a PAR. The information in brackets is variable information that the expert system completes as it is executing.

```
DISPLAY terminal id par
     NETWORK TERMINAL IDS         PAR NO. [total pars (2,0)]

     LOCATION: [location name]
     SUBJECT:  DATA COMMUNICATIONS REVIEW
     DATE PAR SUBMITTED: [date pars submitted]
     PAR SUBMITTED TO: [pars submitted to]

     The network being reviewed has a method of identifying
     authorized terminals from unauthorized terminals.
     However, this feature is not being used.  This would
     allow unauthorized devices to be added to the network,
     which increases the likelihood of unauthorized access
     to the system and makes network maintenance more
     difficult.

          We recommend the feature to identify authorized
          terminals be used.
```

Figure 5. Example PAR DISPLAY Statement

Determine the Audit Opinion

The expert system has implemented the feature that determines the audit opinion by maintaining a counter that is incremented each time a PAR is documented. Figure 6 on the next page shows how this is accomplished in a rule. As part of the conclusion of the rule, the variable "total opinion" is incremented by adding 1. This increment can vary based on the severity of the exception. The variable "total pars" is used to keep track of how many PARs have been written. The variable "total pars" is always incremented by 1.

The amount the counter is incremented varies depending on the severity of the PAR. As designed, it could range from zero with no upward limit. The smallest increment used in the expert system was .5 and the largest was 2. For simplicity, these increments were determined during the expert system development phase by the author, who has experience with the significance of the various audit exceptions. A better approach would be to survey several expert data communications auditors and compute an average rating for each exposure. This has been left for future work.

```
RULE 170 to tell if terminal ids not used
IF   control or routing tables are used
AND  NOT updates and access to control and routing tables is
         adequate
THEN control table usage reviewed
AND  total opinion := total opinion + 1
AND  total pars := total pars + 1
AND  ASK workpaper reference for control table description
AND  FILE control table par w
AND  FILE control table par r
AND  DISPLAY control table par
```

Figure 6. Example Rule With Opinion Calculation

Each of the three opinions have an associated counter range. These ranges were also determined during the expert system development phase by the author. The ranges for the opinions are shown in Table I on the next page.

The opinion that is determined corresponds to the range the opinion counter falls within. For example, if the counter is 3.5 the opinion is strong. For simplicity, these ranges were determined by the author based on his experience with data communications audits. A better approach would be to obtain an average of the ratings of several expert auditors. This has been left for future work.

The production rules that determine the opinion are similar to the one shown in Figure 7. The display named "adequate r" is shown to the user if the opinion counter falls in the range from 2.5 up to 8. Figure 8 on the next page shows the "adequate r" display.

TABLE I

AUDIT OPINION RANGES

Audit Opinion	Starting Value	Ending Value
Strong	0.00	2.49
Adequate	2.50	7.99
Weak	8.00	Infinity

```
RULE 430 to tell if opinion stated is adequate
IF   total opinion >= 2.5
AND  total opinion <  8
THEN opinion stated
AND  DISPLAY adequate
AND  FILE adequate r
```

Figure 7. Example of Opinion Generating Rule

```
DISPLAY adequate r

                                   [date pars submitted]


     [pars submitted to]
     [location name]


                         DATA COMMUNICATIONS REVIEW
                              [location name]


     All controls have been reviewed.  Based on the
     findings, the overall opinion for data communications
     is an adequate control environment.  Detailed audit
     comments are attached for your review.

     Your response to the detail comments is requested
     within sixty days.
```

Figure 8. Example Opinion DISPLAY Statement

System Testing

The expert system was tested during development using the unit test method. The goal of the unit test was to assure all statements of all rules were executed and that they performed as designed.

The next phase of testing was conducted after all system development was completed. This phase is normally called a system test. Its purpose was to test the system in as near to actual audit conditions as possible. Actual field testing of the system was not conducted because it could not be coordinated with the audit schedule for 1989.

The system test was completed by using five sets of audit workpapers as a basis for test data. The test data was entered into the system which produced a set of workpapers and an audit report for each test. The workpapers and audit reports generated by the tests can be found in Appendix C - Workpaper Test Results and Appendix D - Audit Report Test Results. The author was involved with three of these audits. The other two were completed by other EDP auditors.

The test results were compared to the actual audit findings that were generated by the auditor who performed the audit. The comparisons that were completed were the following:

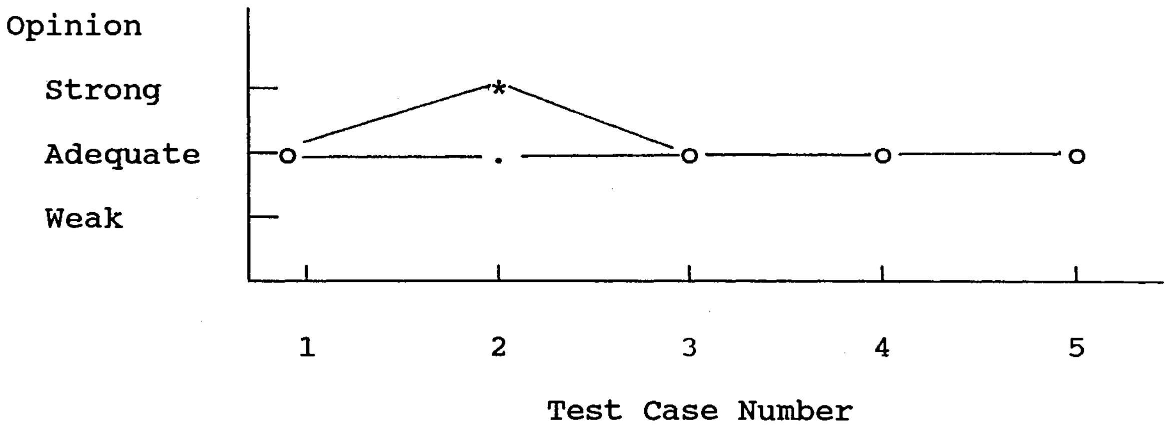
- Opinions
- Total Number PARs
- Number of PARS That Were the Same
- Number of PARs That Were Different

Table II on the following page lists the results of the comparison. Following the table the results are also shown graphically in Figures 9, 10, and 11. Figure 9 shows a comparison of the opinions generated by the expert system and the auditor. Figure 10 shows a comparison of the total number of PARs generated by the expert system and the auditor. Figure 11 shows a comparison of the PARs that were not found by both the expert system and the auditor. Following Table II and the graphs, each of the five tests are described with an explanation of any variances between the expert system and actual results.

TABLE II

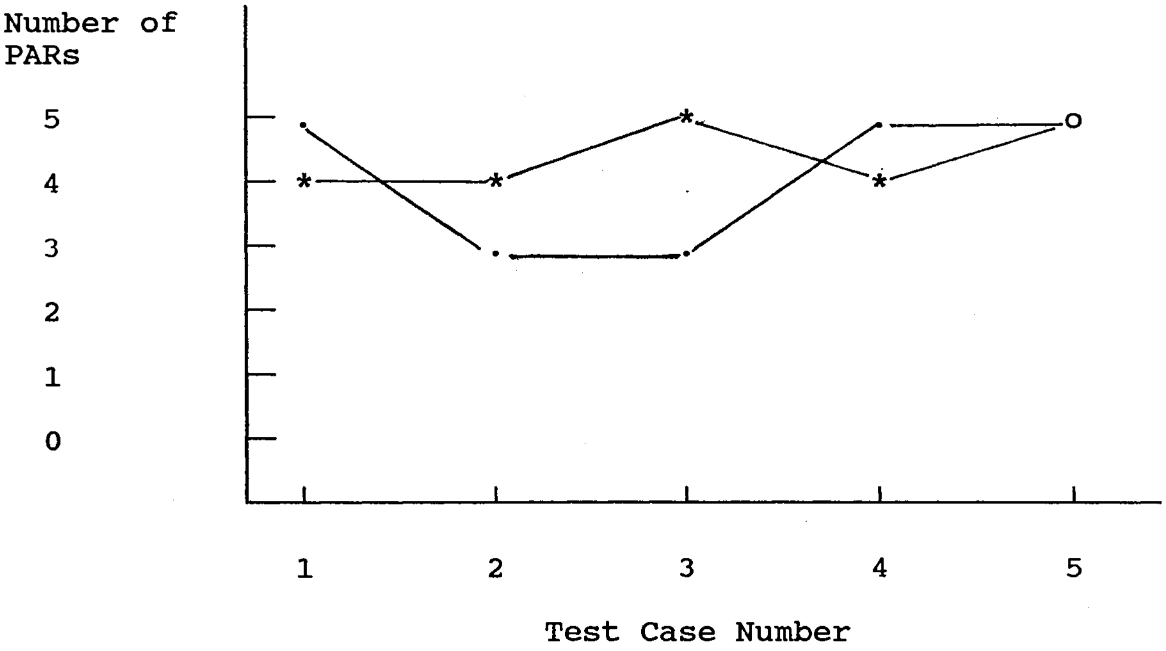
SYSTEM TEST RESULTS COMPARISON

Comparison	Actual	Test
Test 1		
Opinions	Adequate	Adequate
Total Number PARs	4	5
PARS That Were the Same	4	4
PARs That Were Different	0	1
Test 2		
Opinions	Strong	Adequate
Total Number PARs	4	3
PARS That Were the Same	4	3
PARs That Were Different	0	0
Test 3		
Opinions	Adequate	Adequate
Total Number PARs	5	3
PARS That Were the Same	5	3
PARs That Were Different	0	0
Test 4		
Opinions	Adequate	Adequate
Total Number PARs	4	5
PARS That Were the Same	4	5
PARs That Were Different	0	0
Test 5		
Opinions	Adequate	Adequate
Total Number PARs	5	5
PARS That Were the Same	5	5
PARs That Were Different	0	0



* - Actual Audit Data
. - Expert System Choice
o - Actual and Expert System are identical

Figure 9. Graph of Opinion Comparison



* - Actual Audit Data
. - Expert System Choice
o - Actual and Expert System are identical

Figure 10. Graph of Number of PARs Comparison

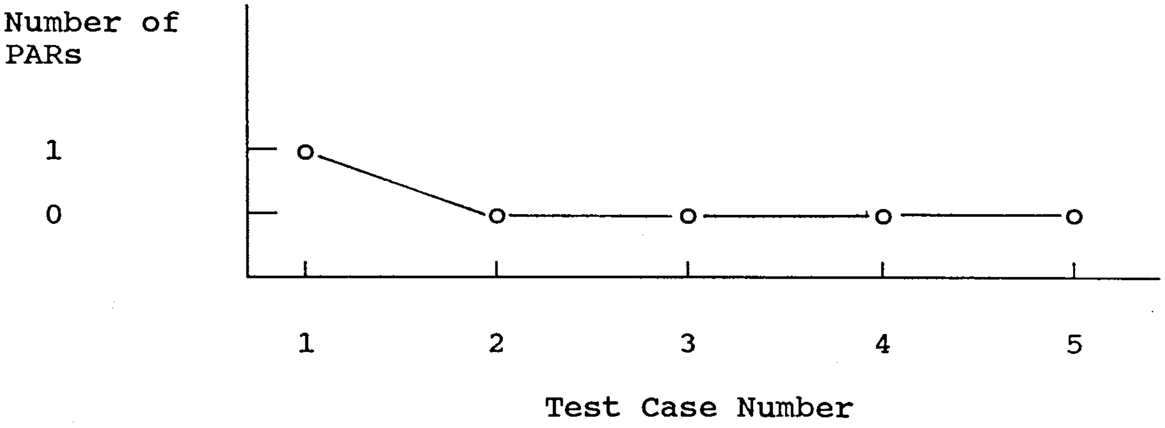


Figure 10. Graph of PARs That Were Different Comparison

Test 1

The first set of test data resulted in receiving the same opinion in both systems and most of the PARs were a one-for-one match. The expert system found one additional PAR which was a valid finding. The original auditor had noted the problem in the workpapers, but chose not to write a PAR because the group being audited had already initiated a corrective action prior to the audit. The findings were similar, but the expert system PARs did not contain the same level of explanation for the finding and exposure.

Test 2

The second test found the same problems as in the actual audit. The number of PARs differ because when they were written they were grouped differently. The audit opinions were different. The expert system gave an adequate because it did not assess the significance of the PARs to this particular audit. A particular finding may vary in importance depending on the type of network. Again, the system found basically the same findings as the actual audit data.

Test 3

The third test resulted in an adequate opinion for both the expert system and the actual audit data. The same areas of exposure were identified by both. The difference in the number of PARs is due to the way the PARs were written. The expert system treated the problem as one item with multiple subparts, where in the actual audit it was written as separate PARs.

Test 4

The fourth test resulted in an adequate opinion for both the expert system and the actual audit data. The same areas of exposure were identified by both. This time it was the expert system that had two PARs for the same exposures that were covered in one PAR in the actual audit data.

Test 5

The fifth test resulted in an adequate opinion for both the expert system and the actual audit data. Five PARs covering the same exposures were found in both the actual and the test. Once again, this was not a one-per-one match due to grouping the PARs differently.

Recap

The expert system did a good job of identifying the correct opinion in most cases. In four of the five test cases, the same audit opinion was reached. In the case where a different opinion was given, it was due to the expert system giving a high level of significance to a finding that, in this case, was a minor problem. This points out a need for the expert system to provide a measure of sensitivity for at least some of the exposures being reviewed.

The outcome of the testing in relation to PARs is very good, since the same exposures were found in almost all cases. There was only one exposure that the expert system found that had purposely been ignored by the auditor performing the audit. This does not really present a problem since the auditor should always review the findings of the expert system and agree with them before distributing them to the audit client.

Another factor identified was the PARs generated by the expert system generally did not have as detailed a description of the finding, exposure, and recommendation. This is because the the expert system obtains less background information relating to an exposure than that generally obtained by an auditor. The PAR as written by the expert system is still useful. It provides a template for adding specifics. This can help achieve more uniform PARs.

Writing style also played a role in causing the difference in the number of PARs written. Again, while the expert system may not be able to write a final copy PAR, it can provide the framework that will cause exposures to consistently be segregated in the same PARs from one audit to the next.

One of the things discovered while testing the program is that it is sometimes necessary to answer a question as "not applicable". This feature has not been included in the system. It would be possible to allow for this option using Insight 2 + production rule language.

Another feature that would make the system more user friendly would be to allow the user to change their answers to questions. This would occur in a field situation. The auditor might get inaccurate information that is later corrected.

To do this, there would probably need to be a menu system added to the knowledge data base that would allow the system to forget the facts associated with a particular question. This would cause the system to prompt the user and to process through the knowledge base with the new user responses.

User Training

In the author's opinion the Insight 2 + based expert system is relatively easy to use, so little user training is needed. Ease of use would be evaluated during field testing. Some basic instruction on the use of the various PF keys is useful. This instruction has been included in the expert system title screen. A copy of this title screen can be found at Appendix E.

Operations and Maintenance

The system is operated by the user by responding to questions from the expert system. As the user progresses, their responses are recorded and they are shown any potential audit exceptions. When the goal of reviewing all areas has been reached, the system stops. The user must then run a basic program to create the workpaper and report files. The auditor should review the PARs generated by the system and, as necessary, make adjustments to the PARs to more completely describe the findings, exposures, and recommendations.

Expert system maintenance has been made easier by segregating each area of questions into a separate knowledge base. Also, common control issues are segregated within each knowledge base. This should make it easier to determine what portion of the knowledge base needs updating.

The modularity of the knowledge base makes maintenance easier for several reasons. First, mistakes can affect less of the system. Only facts that have been declared as "shared" can be affected by another module. This reduces the time it takes to test the system after a change, since less of it will need to be tested. Second, the smaller size of modules relative to one large knowledge base reduces the time it takes to edit and compile the knowledge base.

CHAPTER IV

CONCLUSION AND FUTURE WORK

Conclusion

Today, computers are being widely used by the audit profession. This has led to the use of electronic spreadsheets, word processors, data base applications, and E-mail. A relatively new field is the development of audit expert systems. These systems automate the audit process by analyzing audit data and generating recommendations. These systems have many potential benefits, including the following:

- Reduced cost
- Faster audits
- Higher quality audits
- More consistent quality
- New auditor training
- Providing time for new services
- Preservation of expertise

This study determined the features needed in an expert system that will be used by internal auditors and implemented these features by developing an expert system for auditing data communications networks. The features needed in an audit expert system are the following:

- Collect and evaluate audit evidence
- Document user input
- Process uncertain user input
- Explain why conclusions are drawn in a way that will train new auditors
- Identify audit exceptions and determine which should go in the final report
- Determine the audit opinion

These features were implemented in an expert system that can be used to assist an EDP auditor in performing an audit of a data communications network. Testing of the system showed that it could find the same exposures as an auditor using an "audit program" as a guide.

There were some differences between the actual audit data and that generated by the expert system, but most of these were minor differences. Some differences could be resolved through further enhancement of the knowledge base. Enhancement of the data base is planned to allow for changes in the audit profession.

One area in which the expert should be especially helpful is the training of new auditors. The explanation facility is a vast improvement over what auditors would have to do to research a question in an "audit program".

Another positive aspect of the system is that it should help achieve consistency in findings, recommendations, and opinions. Furthermore, since the findings are drafted, it should speed up the administrative task of writing the PARs and audit report.

It is worth noting the Insight 2 + expert system shell functioned well during the study. It had good diagnostic features and many advanced features that were useful in implementing the system.

Future Work

There are several areas where additional work could be performed. One area would be to arrange to test the system in the field using live audit data and personnel with varying levels of experience in both the EDP audit profession and in performing data communications audits. This would more thoroughly test the system and probably result in additional enhancements to the system.

Another area where work could be done would include development of additional knowledge bases with specific rules for reviewing IBM, DEC, HP, and LAN networks. These areas will not always need to be reviewed in a data communications audit so they can be run via the Insight 2 + CHAIN command, depending on user responses to queries from the main knowledge base.

Another useful, but nonessential, feature that could be added to the system is a menu system for skipping from one part of the knowledge base to another. This menu system could also simplify the process of saving the expert system responses when a user wants to stop in the middle of the session.

Two more possible features would be to allow "not applicable" to be answered to a question so that it could be skipped and to provide access to a text editor while answering a question so an explanatory note could be written.

Another feature would be to create a data base that would show how often each audit finding has been found in previous audits. This would provide the expert system user with some measure of the frequency an exposure is cited.

REFERENCES

1. Abdolmohammadi, Mohammad J. Decision Support and Expert Systems in Auditing: A Review and Research Directions. Accounting and Business Research 17, 66 (Spring 1987), 173-185.

2. Borthick, A. Faye Artificial Intelligence in Auditing: Assumptions and Preliminary Development. Advances in Accounting 5, (1987), 179-204.

3. Chu, Grace T. Expert Systems in Computer Based Auditing. The EDP Auditor Journal 1, (1989), 25-35.

4. Colligan, Francis J., Allman, Gregory, L. Artificial Intelligence and Expert Systems for Accounting and Auditing. Corporate Accounting 4, (Winter 1986), 83-87.

5. Connell, N. A. D. Expert Systems in Accountancy: A Review of Some Recent Applications. Accounting and Business Research 17, 67 (Summer 1987), 221-233.

6. Dungan, Chris W., Chandler, John S. Auditor: A Microcomputer-based Expert System to Support Auditors in the Field. Expert Systems 2, 4 (Oct. 1985), 210-221.

7. Ford, John C. Expert Systems in Auditing. Expert Systems Planning/Implementation/Integration 1, 1 (Spring 1989), 49-54.

8. Garner, B. J., Tsui, E. Recent Advances in Computer Audit Research. The EDP Auditor Journal 4, (1985), 3-16.

9. Hayes-Roth, Frederick, Waterman, Donald A., and Lenat, Douglas B., eds. Building Expert Systems. Addison-Wesley, Reading, Massachusetts, 1983.

10. Hink, Robert F., Woods, David L. How Humans Process Uncertain Knowledge: An Introduction for Knowledge Engineers. AI Magazine 8,3 (Fall 1987), 41-53.

11. McKee, Thomas E. Expert Systems: The Final Frontier? CPA Journal (Jul. 1986), 42-46.

12. Martin, James, Building Expert Systems a Tutorial. Prentice Hall, Englewood Cliffs, New Jersey, 1988.

13. Temkin, Robert H. Automating Auditing: Auditing Will Never Be the Same. Corporate Accounting 4, (Fall 1986), 56-59.

14. Wick, Michael R., Slagle, James R. An Explanation Facility for Today's Expert Systems. IEEE Expert (Spring 1989), 26-36.

APPENDIX A

AUDIT PROGRAM

DATA COMMUNICATIONS AUDIT PROGRAM

I. AUDIT OBJECTIVES

A. The data communications system (or network) directly affects the computing environment by determining who can access a computing resource. Appropriate controls must be in place to prevent unauthorized use or disruption of the data network.

B. Data transported throughout a communications network is vulnerable to a variety of exposures, from unauthorized disclosure to lost or corrupted data, because of network failure. Any error in message transmission, reception, or content must be detected. Detected errors must be reported to network operations personnel.

C. Proper controls are needed to preserve data (or message) integrity while under control of the network. The goal of data integrity is to ensure only valid and authorized data can be received or transmitted and that transmitted data is identical to received data.

II. CONTROL ISSUES

A. The makeup of most networks necessitates a network control group. This group should be responsible for the network's continuing operation, resolution of daily problems, and consulting with users on network operation.

B. Access controls are needed for both physical and operational access. Physical controls ensure a secure environment and prevent unauthorized access to network components, such as terminals, modems, communication lines, etc. Operational controls provide a second level of defense by securing communication software, controlling dial-up ports, limiting information displayed on network sign-on screens, and securing user identification codes and passwords.

C. Data authorization is a key element of network security. An authorization process should employ proper checks and approvals before a message is allowed to enter the network.

D. Performance monitoring provides two useful information sources. First, network reliability can be determined from performance data. Network reliability (and thus availability) directly affects data integrity. Second, performance data can be used to generate audit trails, thereby allowing tracing of transactions, reporting accesses, and identifying exception conditions.

III. ADMINISTRATIVE

A. Obtain an organization chart and identify the network manager or owner. What are the responsibilities associated with this position? A general ELIS standard requires telecommunications networks to have a designated owner.

B. Obtain and review network policy statements and associated procedures. Do they cover:

1. Dial-up access using public telephone services? Uncontrolled dial ports make the computer network vulnerable to outside attacks.

2. Home access and other off premises access? Policy and procedures should dictate off premise computing requirements so they can be applied prudently and consistently.

3. Access via intelligent terminals, such as personal computers? Intelligent terminals can store access information to automate host access. Although this may simplify the log-in process, it can create unnecessary exposures.

4. Confidentiality of network access methods? Information such as dial-up telephone numbers, passwords, PINS, etc., must be kept confidential.

5. Other topics to consider which might affect network security and/or operation:

   a. Individuals authorized to access the network.
   b. Individuals who support the network, including administering/monitoring security concerns.
   c. Connections to the network from

uncontrolled locations.

d. Connections to the network by other networks.

e. Encryption of confidential information to protect during transmission and storage.

Note: if documented procedures are not available, describe general practices.

C. Obtain a description of the data communications network. This often comes in the form of a blueprint or similar graphical representation. If the network is extremely large, a graphical description of the network may not be available or even practical to review. The intent of this step is to familiarize yourself with the network - what it does and where it goes.

1. Destination of lines from communications controllers.
2. Port address, type, location, etc., for all dial-up access.

D. Determine if peer network security reviews are performed.

E. Are suspected security violations passed on to a security officer and (when appropriate) the Regional EDP Audit Manager for resolution?

F. Is there a policy established requiring that users log off before leaving a terminal?

G. Is the network used to restrict access to particular terminals during scheduled business hours? Is supervisory approval needed to bring a terminal up outside scheduled operating hours? How is this controlled?

H. Are there written procedures to follow for starting and stopping the network?

I. Is an operations manual available which cross-references error messages and suggested corrective actions?

J. Describe procedures used to maintain network nodes, such as the addition of new nodes and removal of inactive nodes.

K. Obtain a description of the addressing scheme used by the network. An understanding of how CPUs know which terminals they are communicating to can aid in understanding and defining audit trails.

L. What procedures are in place to control both company and non-company personnel (such as customers, contractors, business partners, suppliers, etc.) who may have authorized access to specific nodes in the network? Consider the following:

1. Requirements for granting access to the network.
2. Monitoring the need for continued access.
3. Revocation of network access when no longer needed. This includes returning RPG and Secure ID Cards, suspension of network account codes and passwords, and disabling auto-callback devices.

M. Are network facilities such as trace, diagnostic, and monitor adequately controlled? Are any associated sensitive data files protected?

Note: Network support personnel generally have powerful privileges which might be easily used to obtain confidential information. For example: most network diagnostic tool kits include trace facilities. Tracing data on a communication line can reveal user account codes, passwords, and other confidential information. Access to these tools should be limited to only those individuals whose job function requires such access.

IV. NETWORK ACCESS CONTROL

A. Identify controls in place to authenticate network users. In particular, review dial-up access to the network.

1. Describe the type of dial-up access allowed.

2. If dial-up ports are allowed, how are they controlled? Some methods for controlling include:
   a. Manual controls - operator enabled/disabled modems or ports.
   b. Auto-callback modems.
   c. Auto-callback systems - such as DEFENDER II.
   d. Personal identification devices - such as Secure ID Card or Micro-Frame's Passkey, a random password generator (RPG).
   e. PBX controlled numbers.
   f. Terminal identification via information encoded in the terminal hardware.

Note: Unprotected dial ports expose the network, and thus the host computing facilities, to access attempts by unauthorized individuals (defined to include company and non-company personnel). A key word here is access attempts. In most cases, the "hacker" must pass through the host's own access control security, such as an account code and password. This might offset the need for network access controls in some cases, but also places added emphasis on strong host access control security to prevent break-ins.

Note2: A second concern deals with audit trails. If someone is trying to break in, sufficient information may not be available to identify who. Further, if a break-in attempt is successful, knowledge of what transpired (including potential damage) may never surface.

Note3: Dial-up and callback control mechanisms are vulnerable to call forwarding and call transfer. Generally, additional controls are needed from the PBX service to disable these special phone features.

B. What type of control tables are used to support the network? Consider the following:

1. Password tables used to verify the calling party on network servers, host computers, or other communications servers.
   a. Are passwords encrypted during storage and transmission?
   b. Review other characteristics about password usage, selection, definition, etc.

2. Routing or pooling tables used to selectively route traffic through the network.

Identify where the tables reside and their format. How are the tables maintained? What controls protect the tables from unauthorized access, including individuals responsible for maintenance.

C. Are terminals defined to specific applications or hosts?

V. <u>NETWORK HARDWARE AND SOFTWARE CONTROLS</u>

A. Are alternative facilities available when communication failures occur?

B. Are scrambling or encryption techniques used?

C. Are backup modems maintained at critical communication points?

D. For communications controller software:

1. Are there procedures to activate/deactivate lines?
2. What line protocols are permitted?
3. Identify controller software types in use.
4. Determine whether security is adequate over access and changes.

E. For network communications software:

1. Identify types in use.
2. Determine whether security is adequate over access and changes.

F. Are network facilities secured and physical access limited to authorized persons? Network facilities include wiring cabinets, telephone closets, switching rooms, etc., in office buildings and any other facility involved in data communications. A representative review of these areas may be appropriate.

G. Are all communication software libraries:

1. Protected against unauthorized access?
2. Backed up on a regular basis?

VI. <u>NETWORK PERFORMANCE MONITORING</u>

A. Identify transmission logs.

1. Do they cover transmission errors?
2. Do they cover time capacity problems?

B. Is the network control log reviewed for operator activities?

C. Are line usage records, diagnostic messages, and processing statistics maintained?

D. How are lines selected for performance requirements and specific uses?

E. Are modems equipped with loop-back switches which help determine whether a failure or an increase in errors is being caused by the modem itself or the line to which the modem is connected?

APPENDIX B

LOG PROGRAM LISTING

LOG PROGRAM LISTING

```
 10 OPEN "I",1,"C:\PRL\OPIN.ASC"
 20 OPEN "O",2,"C:\PRL\TEMP.ASC"
 30 COLOR 15,1,1
 40 CLS
 50 PRINT," "
 60 PRINT," "
 70 PRINT,"Please wait while audit report and workpapers
           are being created"
 80 IF EOF(1) GOTO 130
 90 LINE INPUT#1,A$
100 IF EOF(1) GOTO 130
110 PRINT#2,A$
120 GOTO 90
130 CLOSE #1
140 OPEN "I",1,"C:\PRL\RPTA.ASC"
150 IF EOF(1) GOTO 200
160 LINE INPUT#1,A$
170 IF EOF(1) GOTO 200
180 PRINT#2,A$
190 GOTO 160
200 CLOSE #1
210 OPEN "I",1,"C:\PRL\RPTB.ASC"
220 IF EOF(1) GOTO 270
230 LINE INPUT#1,A$
240 IF EOF(1) GOTO 270
250 PRINT#2,A$
260 GOTO 230
270 CLOSE #1
280 OPEN "I",1,"C:\PRL\RPTBB.ASC"
290 IF EOF(1) GOTO 340
300 LINE INPUT#1,A$
310 IF EOF(1) GOTO 340
320 PRINT#2,A$
330 GOTO 300
340 CLOSE #1
350 OPEN "I",1,"C:\PRL\RPTC.ASC"
360 IF EOF(1) GOTO 410
370 LINE INPUT#1,A$
380 IF EOF(1) GOTO 410
390 PRINT#2,A$
400 GOTO 370
410 CLOSE #1
420 OPEN "I",1,"C:\PRL\RPTD.ASC"
430 IF EOF(1) GOTO 480
440 LINE INPUT#1,A$
```

```
450 IF EOF(1) GOTO 480
460 PRINT#2,A$
470 GOTO 440
480 CLOSE #1
490 OPEN "I",1,"C:\PRL\RPTE.ASC"
500 IF EOF(1) GOTO 550
510 LINE INPUT#1,A$
520 IF EOF(1) GOTO 550
530 PRINT#2,A$
540 GOTO 510
550 CLOSE #1
560 CLOSE #2
570 OPEN "I",1,"C:\PRL\TEMP.ASC"
580 OPEN "O",2,"C:\PRL\REPORT.ASC"
590 OPEN "O",3,"C:\PRL\WORK.ASC"
600 IF EOF(1) GOTO 720
610 LINE INPUT#1,A$
620 IF EOF(1) GOTO 720
630 B$=MID$(A$,1,1)
640 I=LEN(A$)
650 IF I>0 THEN I=I-1
660 C$=MID$(A$,2,I)
670 I=VAL(B$)
680 IF I=1 THEN GOTO 610
690 IF I=2 THEN PRINT#2,C$
700 IF I<>2 THEN PRINT#3,A$
710 GOTO 610
720 PRINT," "
730 PRINT," "
740 PRINT,"Audit report and workpapers have been created"
750 CLOSE
760 SYSTEM
```

APPENDIX C

WORKPAPER TEST RESULTS

TEST 1

WORKPAPER TEST RESULTS

TEST 1

Subject:	7KTK - Data Communications Review
Site:	TST1
Location:	Test Location 1
Assignment:	TEST01

Audit Work Documentation

ADMINISTRATION

A Network ownership has not been specifically defined. However, the implicit network owner is:

Shared responsibility by system programming staff. See

B-1-1.

B Policy review

B.1 Dial access is allowed on the network. There is a policy that covers dial access control. This policy is referenced at:
B-1-1

B.2 Off premise or home access is allowed and there is a policy covering this type of access. The policy is referenced at:
B-7-2

Off premise or home access is allowed and there is a policy covering this type of access. Compliance with the policy was reviewed and no problems were found. Documentation of the compliance review can be found at:
B-7-2

B.3 Intelligent terminals or PCs are used and there is a policy covering this type of access. The policy is referenced at:
B-8 and B-9

Intelligent terminals or PCs are used and there is a policy covering this type of access. Compliance

to this policy was tested and no problems were found. This documentation is at:
B-9

B.4 A policy exists requiring users to keep network access methods such as phone numbers, userids, and passwords confidential. This policy is referenced at:
B-8 and B-9

A policy exists requiring users to keep network access methods such as phone numbers, userids, and passwords confidential. Several users were reviewed and they are in compliance with the policy. The workpapers for this compliance test can be found at:
B-9

B.5 Inter-connections to other networks are allowed. A policy covering this type of access is available. It is referenced at:
B-1-2

C. You have said there is adequate hardware documentation for routine maintenance of the network hardware and for contingency planning purposes. This documentation is kept current through regular maintenance procedures.

D. There is no peer review of the network. This question is for information only and does not show any control weakness.

E. Network security violations are NOT normally reviewed with auditing. This should be discussed with the audit client to assure them that auditing is available to assist them in researching their security problems. Also, auditing can make security weaknesses and their solutions known to other company sites.

F. There is a policy requiring users to log off a terminal before leaving. See policy referenced at:
B-3

G. There are no terminals where it is feasible to restrict them to specific applications to improve network control.

H. There is good network operator documentation that provides the operator help with error messages, instructions for starting and stopping the network. Operator procedures are referenced at:

B-6-1

There is good network operator documentation and a review of a sample of this documentation shows it is being kept up to date. Compliance testing documentation can be found at:
B-6-2

I. Network update procedures were reviewed and they did not meet the following criteria:

- The update process is well documented.
- A list of approved network hardware has been developed and is maintained as a guideline to network device procurement.
- The update is done in a way that allows a quick return to the previous configuration if there are problems.
- All changes are well commented with the software.

See PAR 1.

J. The addressing scheme is secure and does not allow masquerading as an authorized device. The addressing scheme is documented at:
B-1-4

K. Physical security does not meet all of the following requirements.

- communications equipment is housed in areas where access is limited to appropriate personnel (all equipment except terminals) .
- These areas are locked when no one is present in the area.

This places network integrity and security at risk. See PAR 2.

L. Contractors who work on communications equipment are escorted by company personnel while on site.
B-1-4

M. Monitoring hardware and software usage was reviewed. Its use is not adequately controlled so only authorized individuals have access to trace facilities and data. See PAR 3.

N. Security of network software was reviewed and problems were found. Documentation of this review can be found at:
B-1-6

See PAR 4.

NETWORK ACCESS CONTROL

A. Dial access is allowed on the network. A description of the types of dial access allowed can be found at:
B-1-4

B. There is dial access to the network, but there is adequate host security for the application and data on the network. Thus, dial access security measures are not required.

C. Manual activation/deactivation of lines is not used to protect dial-in lines

See item B above

D. Callback modems are used to protect dial-in lines.

Since callback is used as a method of control, the outgoing ports must be protected from someone calling in on those phone numbers. If this is allowed, they may be able to obtain access without going through the callback procedure. The compliance test found the outgoing ports and modems are adequately protected from this exposure. Documentation of this compliance test can be found at:
B-1-4

E. Random password generators are not used to protect dial-in lines.

See item B above

F. Captive accounts that limit exposure of dial access are not used to protect dial in lines

See item B above

G. PBX/network passwords are not used to protect dial-in lines.

See item B above

H. Other adequate control measures are used to protect dial-in lines.

I. The network being reviewed has a method of identifying authorized terminals from unauthorized terminals and it is being used. For a description of the terminal id method, see the following work-

paper reference:
B-1-5

J. The network being reviewed does not make use of control or routing tables.

NETWORK HARDWARE AND SOFTWARE CONTROLS

A. A contingency plan has not been developed that adequately provides for the recovery of the network in the event of a loss of network availability. A contingency plan should cover the following items:

- list of personnel responsible for developing and maintaining a plan
- list of personnel responsible for completing a recovery
- provisions for off-site backup of software, data, and documentation needed in the recovery
- maintenance of a list of needed spare equipment, or agreements with vendors regarding lead time to replace equipment
- regular test schedule for plan

See PAR 5.

B. Need for backup equipment (spares) has been adequately review and implemented.

C. No scrambling or encryption technique is used.

D. The update procedure for hardware and software for network controllers is adequate to ensure only authorized changes are allowed. For a description of the update procedure see workpaper reference:
B-1-6

NETWORK PERFORMANCE MONITORING

A. The operator log (if applicable) is reviewed regularly for unusual operator activity that could indicate unauthorized activities or that additional training is necessary. An example log can be found at the following workpaper reference:
B-1-8

B. The network hardware and software error log (if applicable) is reviewed regularly to identify potential network problems so corrective action can be initiated if warranted. A sample of this error log can be found at the following workpaper reference:

B-1-8

C. Performance monitoring techniques are used on the network. These are documented at the following workpaper reference:

TEST 2

WORKPAPER TEST RESULTS

TEST 2

Subject: 7KTK - Data Communications Review
Site: TST2
Location: Test Location 2
Assignment: TEST02

Audit Work Documentation
==
ADMINISTRATION

A. Network ownership has been defined. The network owner is:

O. Owner, Senior Analyst, General Purpose Network

Their duties are:

Coordinate all network activities with interested parties.

B. Policy review

B.1 Dial access is allowed on the network. There is a policy that covers dial access control. This policy is referenced at:
B-3

B.2 Off premise or home access is allowed and there is a policy covering this type of access. The policy is referenced at:
B-1-1-1

Off premise or home access is allowed and there is a policy covering this type of access. Compliance with the policy was reviewed and no problems were found. Documentation of the compliance review can be found at:
Step not performed

B.3 Intelligent terminals or PCs are used and there is a policy covering this type of access. The policy is referenced at:
B-3

Intelligent terminals or PCs are used and there is a policy covering this type of access. Compliance to this policy was tested and no problems were found. This documentation is at:
Step not performed

B.4 A policy exists requiring users to keep network access methods such as phone numbers, userids, and passwords confidential. This policy is referenced at:
B-3

There is a policy requiring users to keep network access methods such as phone numbers, userids, and passwords confidential. However, during a review of several users, problems with compliance were noted. Documentation of the compliance test can be found at:
B-3

See PAR 1

B.5 Inter-connections to other networks are allowed. A policy covering this type of access is available. It is referenced at:
B-3

C. You have said there is adequate hardware documentation for routine maintenance of the network hardware and for contingency planning purposes. This documentation is kept current through regular maintenance procedures.

D. There is no peer review of the network. This question is for information only and does not show any control weakness.

E. Network security violations are normally reviewed with auditing.

F. There is a policy requiring users to log off a terminal before leaving. See policy referenced at:
B-3

G. There are no terminals where it is feasible to restrict them to specific applications to improve network control.

H. There is good network operator documentation that provides the operator help with error messages and instructions for starting and stopping the network. Operator procedures are referenced at:
B-7

There is good network operator documentation and a review of a sample of this documentation shows it is being kept up to date. Compliance testing documentation can be found at:
B-7

I. Network update procedures were reviewed and they meet the following criteria:

- The update process is well documented.
- A list of approved network hardware has been developed and is maintained as a guideline to network device procurement.
- The update is done in a way that allows a quick return to the previous configuration if there are problems.
- All changes are well commented with the software.

The update procedures are documented at:
B-4

A compliance test of network update procedures showed they are being followed. See documentation of the test at:
B-4

J. The addressing scheme is secure and does not allow masquerading as an authorized device. The addressing scheme is documented at:
B-1-1-2

K. Physical security meets the following criteria:

- Communications equipment is housed in areas where access is limited to appropriate personnel (all equipment except terminals).
- These areas are locked when no one is present in the area.

See documentation at reference:
B-1-1-4

L. Contractors who work on communications equipment are escorted by company personnel while on site.
B-3

M. Monitoring hardware and software usage was reviewed. Its use is not adequately controlled so only authorized individuals have access to trace facilities and data.

See PAR 2.

N. Security of network software was reviewed and problems were found. Documentation of this review can be found at:
B-1-1-4

See PAR 3.

NETWORK ACCESS CONTROL

A. Dial access is allowed on the network. A description of the types of dial access allowed can be found at:
B-1-1-2

B. There is dial access to the network, but there is adequate host security for the application and data on the network. Thus, dial access security measures are not required.

C. Manual activation/deactivation of lines is not used to protect dial-in lines.
See item B above

D. Callback modems are used to protect dial-in lines

Since callback is used as a method of control, the outgoing ports must be protected from someone calling in on those phone numbers. If this is allowed, they may be able to obtain access without going through the callback procedure. The compliance test found the outgoing ports and modems are adequately protected from this exposure. Documentation of this compliance test can be found at:
B-1-1-2

E. Random password generators are used to protect dial-in lines.

F. Captive accounts that limit exposure of dial access are not used to protect dial-in lines.
See item B above

G. PBX/network passwords are not used to protect dial-in lines.

See item B above

H. Other adequate control measures are not used to protect dial-in lines.

See item B above

I. The network being reviewed has a method of

identifying authorized terminals from unauthorized terminals and it is being used. For a description of the terminal id method see the following workpaper reference:
B-1-1-4

J. The network being reviewed does not make use of control or routing tables.

NETWORK HARDWARE AND SOFTWARE CONTROLS

A. A contingency plan has been developed that adequately provides for the recovery of the network in the event of a loss of network availability. See the following workpaper reference for a description of the plan:
B-3

B. Need for backup equipment (spares) has been adequately reviewed and implemented.

C. No scrambling or encryption technique is used.

D. The update procedure for hardware and software for network controllers is adequate to ensure only authorized changes are allowed. For a description of the update procedure, see workpaper reference:
B-1-1-3

NETWORK PERFORMANCE MONITORING

A. The operator log (if applicable) is reviewed regularly for unusual operator activity that could indicate unauthorized activities or that additional training is necessary. An example log can be found at the following workpaper reference:
B-1-1-3

B. The network hardware and software error log (if applicable) is reviewed regularly to identify potential network problems so corrective action can be initiated if warranted. A sample of this error log can be found at the following workpaper reference:
B-1-1-3

C. Performance monitoring techniques are used on the network. These are documented at the following workpaper reference:
B-1-1-4

TEST 3

WORKPAPER TEST RESULTS

TEST 3

Subject: 7KTK - Data Communications Review
Site: TST3
Location: Test Location 3
Assignment: TEST03

Audit Work Documentation

===

ADMINISTRATION

A. Network ownership has been defined. The network owner is:

Network Owner

Their duties are:

Coordinate network

B. Policy review

B.1 Dial access is allowed on the network. There is a policy that covers dial access control. This policy is referenced at:
B-15

B.2 Off premise or home access is allowed and there is a policy covering this type of access. The policy is referenced at:
B-2

Off premise or home access is allowed and there is a policy covering this type of access. Compliance with the policy was reviewed and no problems were found. Documentation of the compliance review can be found at:
Test not done

B.3 Intelligent terminals or PCs are used and there is a policy covering this type of access. The policy is referenced at:
B-15

Intelligent terminals or PCs are used and there is

a policy covering this type of access. Compliance to this policy was tested and no problems were found. This documentation is at:
Test not done

B.4 A policy exists requiring users to keep network access methods such as phone numbers, userids, and passwords confidential. This policy is referenced at:
B-15

A policy exists requiring users to keep network access methods such as phone numbers, userids, and passwords confidential. Several users were reviewed and they are in compliance with the policy. The workpapers for this compliance test can be found at:
Test not done

B.5 There are no inter-connections to other networks.

C. You have said there is adequate hardware documentation for routine maintenance of the network hardware and for contingency planning purposes. This documentation is kept current through regular maintenance procedures.

D. There is no peer review of the network. This question is for information only and does not show any control weakness.

E. Network security violations are normally reviewed with auditing.

F. There is a policy requiring users to log off a terminal before leaving. See policy referenced at:
B-4

G. There are no terminals where it is feasible to restrict them to specific applications to improve network control.

H. There is good network operator documentation that provides the operator help with error messages and instructions for starting and stopping the network. Operator procedures are referenced at:
B-5

There is good network operator documentation and a review of a sample of this documentation shows it is being kept up to date. Compliance testing documentation can be found at:
B-6

I. Network update procedures were reviewed and they meet the following criteria:

- The update process is well documented.
- A list of approved network hardware has been developed and is maintained as a guideline to network device procurement.
- The update is done in a way that allows a quick return to the previous configuration if there are problems.
- All changes are well commented with the software.

The update procedures are documented at:
B-7

A compliance test of network update procedures showed they are being followed. See documentation of the test at:
Test not done

J. The addressing scheme is secure and does not allow masquerading as an authorized device. The addressing scheme is documented at:
B-7

K. Physical security meets the following criteria:

- Communications equipment is housed in areas where access is limited to appropriate personnel (all equipment except terminals).
- These areas are locked when no one is present in the area.

See documentation at reference:
B-8

L. Contractors who work on communications equipment are escorted by company personnel while on site.
B-3

M. Monitoring hardware and software usage was reviewed. Its use is not adequately controlled so only authorized individuals have access to trace facilities and data.

See PAR 1.

N. Security of network software was reviewed and problems were found. Documentation of this review can be found at:
B-9

See PAR 2.

NETWORK ACCESS CONTROL

A. Dial access is allowed on the network. A description of the types of dial access allowed can be found at:
B-10

B. Dial access is not adequately secured because none of the following types of dial security are used:

- Manual activation/deactivation of dial lines
- Callback modems
- Random password generators
- Captive accounts that limit exposure of dial access
- PBX/network passwords
- Other adequate control measures

See PAR 3.

C. Manual activation/deactivation of lines is not used to protect dial-in lines.

See item B above

D. Callback modems are not used to protect dial-in lines.

See item B above

E. Random password generators are not used to protect dial-in lines.

See item B above

F. Captive accounts that limit exposure of dial access are not used to protect dial-in lines.

See item B above

G. PBX/network passwords are not used to protect dial-in lines.

See item B above

H. Other adequate control measures are not used to protect dial-in lines.

See item B above

I. The network being reviewed has a method of identifying authorized terminals from unauthorized terminals and it is being used. For a description of the terminal id method, see the

following work paper reference:
B-11

J. The network being reviewed does not make use of control or routing tables.

NETWORK HARDWARE AND SOFTWARE CONTROLS

A. A contingency plan has been developed that adequately provides for the recovery of the network in the event of a loss of network availability. See the following workpaper reference for a description of the plan:
B-11

B. Need for backup equipment (spares) has been adequately reviewed and implemented.

C. No scrambling or encryption technique is used.

D. The update procedure for hardware and software for network controllers is adequate to ensure only authorized changes are allowed. For a description of the update procedure, see workpaper reference:
B-12

NETWORK PERFORMANCE MONITORING

A. The operator log (if applicable) is reviewed regularly for unusual operator activity that could indicate unauthorized activities or that additional training is necessary. An example log can be found at the following workpaper reference:
B-13

B. The network hardware and software error log (if applicable) is reviewed regularly to identify potential network problems so corrective action can be initiated if warranted. A sample of this error log can be found at the following workpaper reference:
B-14

C. Performance monitoring techniques are used on the network. These are documented at the following workpaper reference:
B-15

TEST 4

WORKPAPER TEST RESULTS

TEST 4

Subject:	7KTK - Data Communications Review
Site:	TST4
Location:	Test Location 4
Assignment:	TEST04

Audit Work Documentation

ADMINISTRATION

A. Network ownership has been defined. The network owner is:

DECnet owner

Their duties are:

Manage network

B. Policy review

B.1 Dial access is allowed on the network, but there is no policy that covers dial access control. The network contains sensitive applications that need protection.

See PAR 1.

B.2 Off premise or home access is allowed and there is a policy covering this type of access. The policy is referenced at:
B-2

Off premise or home access is allowed and there is a policy covering this type of access. Compliance with the policy was reviewed and no problems were found. Documentation of the compliance review can be found at:
Test not done

B.3 Intelligent terminals or PCs are used and there is a policy covering this type of access. The policy is referenced at:
B-3

Intelligent terminals or PCs are used and there is a policy covering this type of access. Compliance to this policy was tested and no problems were found. This documentation is at:
Test not done

B.4 There is no policy requiring users to keep network access methods such as phone numbers, userids, and passwords confidential.

See PAR 2

B.5 There are no inter-connections to other networks.

C. You have said there is adequate hardware documentation for routine maintenance of the network hardware and for contingency planning purposes. This documentation is kept current through regular maintenance procedures.

D. There is no peer review of the network. This question is for information only and does not show any control weakness.

E. Network security violations are normally reviewed with auditing.

F. There is a policy requiring users to log off a terminal before leaving. See policy referenced at:
B-5

G. There are no terminals where it is feasible to restrict them to specific applications to improve network control.

H. There is good network operator documentation that provides the operator help with error messages and instructions for starting and stopping the network. Operator procedures are referenced at:
B-6

There is good network operator documentation and a review of a sample of this documentation shows it is being kept up to date. Compliance testing documentation can be found at:
B-7

I. Network update procedures were reviewed and they meet the following criteria:

- The update process is well documented.
- A list of approved network hardware has been developed and is maintained as a guideline to

network device procurement.

- The update is done in a way that allows a quick return to the previous configuration if there are problems.
- All changes are well commented with the software.

The update procedures are documented at:
B-6

A compliance test of network update procedures showed they are being followed. See documentation of the test at:
B-6

J. The addressing scheme is secure and does not allow masquerading as an authorized device. The addressing scheme is documented at:
B-7

K. Physical security meets the following criteria:

- Communications equipment is housed in areas where access is limited to appropriate personnel (all equipment except terminals).
- These areas are locked when no one is present in the area.

See documentation at reference:
B-8

L. Contractors who work on communications equipment are escorted by company personnel while on site.
B-8

M. Monitoring hardware and software usage was reviewed. Its use is controlled so only authorized personnel can trace data. The types of monitoring being used can be found at:
B-9

N. Security of network software was reviewed and no problems were found. Documentation of this review can be found at:
B-10

NETWORK ACCESS CONTROL

A. Dial access is allowed on the network. A description of the types of dial access allowed can be found at:
B-11

B. Dial access is not adequately secured because none of the following types of dial security are used:

- Manual activation/deactivation of dial lines
- Callback modems
- Random password generators
- Captive accounts that limit exposure of dial access
- PBX/network passwords
- Other adequate control measures

See PAR 3.

C. Manual activation/deactivation of lines is not used to protect dial-in lines.

See item B above

D. Callback modems are not used to protect dial-in lines.

See item B above

E. Random password generators are not used to protect dial-in lines.

See item B above

F. Captive accounts that limit exposure of dial access are not used to protect dial-in lines.

See item B above

G. PBX/network passwords are not used to protect dial-in lines.

See item B above

H. Other adequate control measures are not used to protect dial-in lines.

See item B above

I. The network being reviewed has no method of identifying authorized terminals from unauthorized terminals.

J. The network being reviewed does make use of control or routing tables. These tables are not adequately protected from unauthorized access and update. For a description of the control/routing table usage, see the following workpaper reference:
B-11

See PAR 4.

NETWORK HARDWARE AND SOFTWARE CONTROLS

A. A contingency plan has been developed that adequately provides for the recovery of the network in the event of a loss of network availability. See the following workpaper reference for a description of the plan:
B-12

B. Need for backup equipment (spares) has been adequately reviewed and implemented.

C. No scrambling or encryption technique is used.

D. The update procedure for hardware and software for network controllers is adequate to ensure only authorized changes are allowed. For a description of the update procedure see workpaper reference:
B-13

NETWORK PERFORMANCE MONITORING

A. There is an operator log, but it is not reviewed regularly to identify unauthorized activity or the need for additional training. A regular review of the log could reduce the exposure to loss of service through operator error or unauthorized activity. An example log can be found at the following workpaper reference:
B-14

See PAR 5.

B. The network hardware and software error log (if applicable) is reviewed regularly to identify potential network problems so corrective action can be initiated if warranted. A sample of this error log can be found at the following workpaper reference.
B-15

C. Performance monitoring techniques are used on the network. These are documented at the following workpaper reference:
B-16

TEST 5

WORKPAPER TEST RESULTS

TEST 5

Subject: 7KTK - Data Communications Review
Site: TST5
Location: Test Location 5
Assignment: TEST05

Audit Work Documentation

===

ADMINISTRATION

A. Network ownership has not been specifically defined. However, the implicit network owner is:

System Programming Group

B. Policy review

B.1 Dial access is allowed on the network. There is a policy that covers dial access control. This policy is referenced at:
B-3

B.2 Off premise or home access is not allowed.

B.3 Intelligent terminals or PCs are not used on the network.

B.4 A policy exists requiring users to keep network access methods such as phone numbers, userids, and passwords confidential. This policy is referenced at:
B-5

A policy exists requiring users to keep network access methods such as phone numbers, userids, and passwords confidential.

Several users were reviewed and they are in compliance with the policy. The workpapers for this compliance test can be found at:
Test not completed

B.5 There are no inter-connections to other networks.

C. You have said there is adequate hardware documentation for routine maintenance of the network hardware and for contingency planning purposes. This documentation is kept current through regular maintenance procedures.

D. There is no peer review of the network. This question is for information only and does not show any control weakness.

E. Network security violations are normally reviewed with auditing.

F. There is a policy requiring users to log off a terminal before leaving. See policy referenced at:
Not applicable since there are no terminals

G. There are no terminals where it is feasible to restrict them to specific applications to improve network control.

H. There is good network operator documentation that provides the operator help with error messages and instructions for starting and stopping the network. Operator procedures are referenced at:
B-5

There is good network operator documentation and a review of a sample of this documentation shows it is being kept up to date. Compliance testing documentation can be found at:
B-5

I. Network update procedures were reviewed and they did not meet the following criteria:

- The update process is well documented.
- A list of approved network hardware has been developed and is maintained as a guideline to network device procurement.
- The update is done in a way that allows a quick return to the previous configuration if there are problems.
- All changes are well commented with the software.

See PAR 1.

J. The addressing scheme is secure and does not allow masquerading as an authorized device. The addressing scheme is documented at:
B-7

K. Physical security meets the following criteria:

- Communications equipment is housed in areas where access is limited to appropriate personnel (all equipment except terminals).
- These areas are locked when no one is present in the area.

See documentation at reference:
B-8

L. Contractors who work on communications equipment are escorted by company personnel while on site.
B-9

M. Monitoring hardware and software usage was reviewed. Its use is not adequately controlled so only authorized individuals have access to trace facilities and data.

See PAR 2.

N. Security of network software was reviewed and problems were found. Documentation of this review can be found at:
B-8

See PAR 3.

NETWORK ACCESS CONTROL

A. Dial access is allowed on the network. A description of the types of dial access allowed can be found at:
B-9

B. Dial access is not adequately secured because none of the following types of dial security are used:

- Manual activation/deactivation of dial lines
- Callback modems
- Random password generators
- Captive accounts that limit exposure of dial access
- PBX/network passwords
- Other adequate control measures

See PAR 4.

C. Manual activation/deactivation of lines is not used to protect dial-in lines

See item B above

D. Callback modems are not used to protect dial-in lines.

See item B above

E. Random password generators are not used to protect dial-in lines.

See item B above

F. Captive accounts that limit exposure of dial access are not used to protect dial-in lines.

See item B above

G. PBX/network passwords are not used to protect dial-in lines.

See item B above

H. Other adequate control measures are not used to protect dial-in lines.

See item B above

I. The network being reviewed has no method of identifying authorized terminals from unauthorized terminals.

J. The network being reviewed does not make use of control or routing tables.

NETWORK HARDWARE AND SOFTWARE CONTROLS

A. A contingency plan has been developed that adequately provides for the recovery of the network in the event of a loss of network availability. See the following workpaper reference for a description of the plan:
B-10

B. Need for backup equipment (spares) has been adequately review and implemented.

C. No scrambling or encryption technique is used.

D. The update procedure for hardware and software for network controllers is adequate to ensure only authorized changes are allowed. For a description of the update procedure, see workpaper reference:
B-4

NETWORK PERFORMANCE MONITORING

A. There is an operator log, but it is not reviewed regularly to identify unauthorized activity or the need for additional training. A regular review of the log could reduce the exposure to loss of service through operator error or unauthorized activity. An example log can be found at the following workpaper reference:
B-6

See PAR 5.

B. The network hardware and software error log (if applicable) is reviewed regularly to identify potential network problems so corrective action can be initiated if warranted. A sample of this error log can be found at the following workpaper reference:
B-11

C. Performance monitoring techniques are used on the network. These are documented at the following workpaper reference:
B-12

APPENDIX D

AUDIT REPORT TEST RESULTS

TEST 1

AUDIT REPORT TEST RESULTS

TEST 1

June 2, 1989

Test Auditee 1
Test Location 1

DATA COMMUNICATIONS REVIEW
Test Location 1

All controls have been reviewed. Based on the findings, the overall opinion for data communications is an adequate control environment. Detailed audit comments are attached for your review.

Your response to the detail comments is requested within sixty days.

NETWORK UPDATE PROCEDURES PAR NO. 1

LOCATION: Test Location 1
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 1

Network update procedures were reviewed and they did not meet the following criteria:

- The update process is well documented.
- A list of approved network hardware has been developed and is maintained as a guideline to network device procurement.
- The update is done in a way that allows a quick return to the previous configuration if there are problems.
- All changes are well commented with the software.

Documentation of the update procedures helps all interested parties know what their role in the process is. This can reduce the number problems associated with changes to the network.

We recommend network update procedures be documented.

NETWORK PHYSICAL SECURITY PAR NO. 2

LOCATION: Test Location 1
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 1

Physical security was reviewed. It does not meet all of the following requirements:

- Communications equipment is housed in areas where access is limited to appropriate personnel (all equipment except terminals).
- These areas are locked when no one is present in the area.

This places network integrity and security at risk.

We recommend network devices be stored in areas with limited access whenever possible. If it is not cost justifiable to protect them currently, consideration should be given when other refurbishing of the area is planned.

ACCESS TO MONITORING FACILITIES PAR NO. 3

LOCATION: Test Location 1
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 1

Monitoring hardware and software usage was reviewed. It has a valid system use in resolving network problems, but it could also be used to obtain unauthorized access to confidential data or userids and passwords. Its use is not adequately controlled so only authorized individuals have access to monitoring facilities and data.

We recommend procedures be established to protect the trace hardware and software so unauthorized access would be less likely.

NETWORK SOFTWARE FILE SECURITY PAR NO. 4

LOCATION: Test Location 1
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 1

Security of network software was reviewed and problems were found that too much access was given to some network software files.

We recommend security of network software files be reviewed and be limited on a need to know basis.

CONTINGENCY PLANNING PAR NO. 5

LOCATION: Test Location 1
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 1

A contingency plan has not been developed that adequately provides for the recovery of the network in the event of a loss of network availability. A contingency plan helps assure the network can be reconstructed in a timely manner. A contingency plan should cover items such as the following:

- list of personnel responsible for developing and maintaining a plan
- list of personnel responsible for completing a recovery
- provisions for off-site backup of software, data, and documentation needed in the recovery
- maintenance of a list of needed spare equipment or agreements with vendors regarding lead time to replace equipment
- regular test schedule for plan

We recommend a contingency plan be developed for the network.

TEST 2

AUDIT REPORT TEST RESULTS

TEST 2

June 2, 1989

Test Auditee 2
Test Location 2

DATA COMMUNICATIONS REVIEW
Test Location 2

All controls have been reviewed. Based on the findings, the overall opinion for data communications is an adequate control environment. Detailed audit comments are attached for your review.

Your response to the detail comments is requested within sixty days.

NETWORK ACCESS ROUTINES PAR NO. 1

LOCATION: Test Location 2
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 2

There is a policy requiring users to keep network access methods such as phone numbers, userids, and passwords confidential. Compliance with this policy was reviewed and problems were noted. Failure to keep access methods confidential increases the likelihood someone could obtain unauthorized access to systems on the network.

We recommend all users be informed of the importance of keeping network access routines confidential.

ACCESS TO MONITORING FACILITIES PAR NO. 2

LOCATION: Test Location 2
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 2

Monitoring hardware and software usage was reviewed. It has a valid system use in resolving network problems, but it could also be used to obtain unauthorized access to confidential data or userids and passwords. Its use is not adequately controlled so only authorized individuals have access to monitoring facilities and data.

> We recommend procedures be established to protect the trace hardware and software so unauthorized access would be less likely.

NETWORK SOFTWARE FILE SECURITY PAR NO. 3

LOCATION: Test Location 2
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 2

Security of network software was reviewed and problems were found that too much access was given to some network software files.

> We recommend security of network software files be reviewed and be limited on a need to know basis.

TEST 3

AUDIT REPORT TEST RESULTS

TEST 3

June 2, 1989

Test Auditee 3
Test Location 3

DATA COMMUNICATIONS REVIEW
Test Location 3

All controls have been reviewed. Based on the findings, the overall opinion for data communications is an adequate control environment. Detailed audit comments are attached for your review.

Your response to the detail comments is requested within sixty days.

ACCESS TO MONITORING FACILITIES PAR NO. 1

LOCATION: Test Location 3
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 3

Monitoring hardware and software usage was reviewed. It has a valid system use in resolving network problems, but it could also be used to obtain unauthorized access to confidential data or userids and passwords. Its use is not adequately controlled so only authorized individuals have access to monitoring facilities and data.

> We recommend procedures be established to protect the trace hardware and software so unauthorized access would be less likely.

NETWORK SOFTWARE FILE SECURITY PAR NO. 2

LOCATION: Test Location 3
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 3

Security of network software was reviewed and problems were found that too much access was given to some network software files.

We recommend security of network software files be reviewed and be limited on a need to know basis.

DIAL ACCESS SECURITY PAR NO. 3

LOCATION: Test Location 3
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 3

Dial access is not adequately secured because none of the following types of dial security are used:

- Manual activation/deactivation of dial lines
- Callback modems
- Random password generators
- Captive accounts that limit exposure of dial access
- PBX/network passwords
- Other adequate control measures

Dial access security reduces the likelihood of unauthorized access to sensitive data and applications on the network.

We recommend a review of dial security measures be completed and, if cost effective, dial access security be implemented.

TEST 4

AUDIT REPORT TEST RESULTS

TEST 4

June 2, 1989

Test Auditee 4
Test Location 4

DATA COMMUNICATIONS REVIEW
Test Location 4

All controls have been reviewed. Based on the findings, the overall opinion for data communications is an adequate control environment. Detailed audit comments are attached for your review.

Your response to the detail comments is requested within sixty days.

DIAL ACCESS POLICY PAR NO. 1

LOCATION: Test Location 4
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 4

Dial access is allowed on the network, but no policy has been written covering its control. The corporate computing policy does not require dial access protection. However, this network has sensitive applications that may not be adequately protected by available host security.

Development of a dial access policy that addresses dial access risks may reduce the risk of outside attacks.

> We recommend a dial access policy be developed that addresses the need for greater dial access controls.

NETWORK ACCESS ROUTINES PAR NO. 2

LOCATION: Test Location 4
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 4

There is no policy requiring users to keep network access methods such as phone numbers, userids, and passwords confidential. This increases the likelihood someone could obtain unauthorized access to systems on the network.

> We recommend a policy be adopted to treat network access routines as confidential.

DIAL ACCESS SECURITY PAR NO. 3

LOCATION: Test Location 4
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 4

Dial access is not adequately secured because none of the following types of dial security are used:

- Manual activation/deactivation of dial lines
- Callback modems
- Random password generators
- Captive accounts that limit exposure of dial access
- PBX/network passwords
- Other adequate control measures

Dial access security reduces the likelihood of unauthorized access to sensitive data and applications on the network.

> We recommend a review of dial security measures be completed and, if cost effective, dial access security be implemented.

NETWORK CONTROL TABLE PAR NO. 4

LOCATION: Test Location 4
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 4

The network being reviewed uses control or routing tables. These tables are not adequately protected from unauthorized access and update. This could allow unauthorized changes to be made to the network which could disrupt normal network operations and make future maintenance more difficult.

> We recommend access controls over the control table be reviewed and that access be limited to those who need the access to perform their jobs.

NETWORK OPERATOR LOG PAR NO. 5

LOCATION: Test Location 4
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 4

There is an operator log, but it is not reviewed regularly to identify unauthorized activity or the need for additional training. A regular review of the log could reduce the exposure to loss of service through operator error or unauthorized activity.

> We recommend the operator log be periodically reviewed.

TEST 5

AUDIT REPORT TEST RESULTS

TEST 5

June 2, 1989

Test Auditee 5
Test Location 5

DATA COMMUNICATIONS REVIEW
Test Location 5

All controls have been reviewed. Based on the findings, the overall opinion for data communications is an adequate control environment. Detailed audit comments are attached for your review.

Your response to the detail comments is requested within sixty days.

NETWORK UPDATE PROCEDURES PAR NO. 1

LOCATION: Test Location 5
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 5

Network update procedures were reviewed and they did not meet the following criteria:

- The update process is well documented.
- A list of approved network hardware has been developed and is maintained as a guideline to network device procurement.
- The update is done in a way that allows a quick return to the previous configuration if there are problems.
- All changes are well commented with the software.

Documentation of the update procedures helps all interested parties know what their role in the process is. This can reduce the number problems associated with changes to the network.

We recommend network update procedures be documented.

ACCESS TO MONITORING FACILITIES PAR NO. 2

LOCATION: Test Location 5
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 5

Monitoring hardware and software usage was reviewed. It has a valid system use in resolving network problems, but it could also be used to obtain unauthorized access to confidential data or userids and passwords. Its use is not adequately controlled so only authorized individuals have access to monitoring facilities and data.

We recommend procedures be established to protect the trace hardware and software so unauthorized access would be less likely.

NETWORK SOFTWARE FILE SECURITY PAR NO. 3

LOCATION: Test Location 5
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 5

Security of network software was reviewed and problems were found that too much access was given to some network software files.

We recommend security of network software files be reviewed and be limited on a need to know basis.

DIAL ACCESS SECURITY PAR NO. 4

LOCATION: Test Location 5
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 5

Dial access is not adequately secured because none of the following types of dial security are used:

- Manual activation/deactivation of dial lines
- Callback modems
- Random password generators
- Captive accounts that limit exposure of dial access
- PBX/network passwords
- Other adequate control measures

Dial access security reduces the likelihood of unauthorized access to sensitive data and applications on the network.

We recommend a review of dial security measures be completed and, if cost effective, dial access security be implemented.

NETWORK OPERATOR LOG PAR NO. 5

LOCATION: Test Location 5
SUBJECT: DATA COMMUNICATIONS REVIEW
DATE PAR SUBMITTED: June 2, 1989
PAR SUBMITTED TO: Test Auditee 5

There is an operator log, but it is not reviewed regularly to identify unauthorized activity or the need for additional training. A regular review of the log could reduce the exposure to loss of service through operator error or unauthorized activity.

We recommend the operator log be periodically reviewed.

APPENDIX E

EXPERT SYSTEM TITLE SCREEN

EXPERT SYSTEM TITLE SCREEN

DISPLAY intro

EXPERT SYSTEM FOR

AUDITING DATA COMMUNICATIONS

The following expert system was developed to help auditors conduct an audit of the data communications function. This system's intent is to supplement the knowledge of the auditor by leading the auditor to ask the right questions. The system contains the following features:

- For most questions, the expert system provides an additional explanation of the question by pressing F5. This option is available whenever it is shown on the bottom of the screen. The explanation describes both why the question is being asked and provides additional background information on the question. The explanation facility should be especially helpful to auditors who are not experienced in auditing data communications.

PRESS F1 TO ADVANCE TO THE SECOND PAGE OF THE INTRODUCTION
PRESS F2 TO CONTINUE THE REVIEW
PRESS F10 AND THEN F1 TO EXIT FROM THE SYSTEM

- The system prompts the user to answer questions. Most questions are TRUE/FALSE questions. Some questions ask for entry of a character string, like the name of the location being audited. A third type of question uses a confidence bar to assess whether an answer is TRUE or FALSE. The confidence bar ranges from 0 to 100 representing your confidence that the statement is true. This type of question is asked when the answer is not necessarily 100 percent true or false.

- Be careful not to accidentally hit the escape key, as this will exit from the session and you will have to start over.

- Similarly, avoid the UNKN function key. It has not been programmed into the knowledge base and will cause the system to exit.

- Also, be careful not to use the F3 or F8 key as each of these will cause you to exit the current line of reasoning and restart or go to the menu.

PRESS F1 TO GO TO THE THIRD PAGE OF THE INTRODUCTION
PRESS F2 TO CONTINUE THE REVIEW
PRESS F10 AND THEN F1 TO EXIT FROM THE SYSTEM

- The system will highlight areas where potential problems exist and will make preliminary recommendations in the form of a Preliminary Audit Report (PAR). Each PAR will be marked as to whether it should be included in the final audit report.

- The expert system will also determine the overall audit opinion based on the severity of the findings discovered.

- As stated above, the expert system will recommend both problems to document in a PAR and what the opinion should be for the audit. Both of these are supplied by the system to assist the auditor in completing their review. This feature should help to provide consistency in audit findings and opinions from one audit to the next. However, the auditor and their management should use judgment to determine if they agree with the expert system's findings and opinion.

PRESS F1 TO RETURN TO THE FIRST PAGE OF THE INTRODUCTION
PRESS F2 TO CONTINUE THE REVIEW
PRESS F5 TO GET FURTHER INFORMATION ON A QUESTION
PRESS F10 AND THEN F1 TO EXIT FROM THE SYSTEM

VITA

Patrick D. Fett

Candidate for the Degree of

Master of Science

Thesis: AN EXPERT SYSTEM FOR AUDITING DATA COMMUNICATIONS

Major Field: Computing and Information Sciences

Biographical:

Personal Data: Born in Lima, Ohio, September 16, 1959, the son of Thomas J. and Jennie L. Fett. Married to Lorraine K. Broders on June 2, 1984. Daughter Leah K. Fett, born August 4, 1988.

Education: Graduated from Wapakoneta Senior High School, Wapakoneta, Ohio, in June 1977; received Bachelor of Science Degree in Business Administration from The Ohio State University in June 1982; completed requirements for the Master of Science Degree at Oklahoma State University in July, 1989.

Professional Experience: Accounting Systems Analyst, Conoco, Ponca City, Oklahoma, June 1982 to June 1985. EDP Auditor, E. I. du Pont de Nemours and Company, Ponca City, Oklahoma, July 1985 to present.