INTERNAL CONTROL ASPECTS OF MINICOMPUTER-BASED FINANCIAL ACCOUNTING APPLICATIONS ARISING FROM MINICOMPUTER OPERATING SYSTEMS

Anthony Walsh*

Introduction

The potential internal control problems of minicomputer-based accounting applications are identified in the literature on internal control and audit by reference to the elements of the environment of operation of minicomputers which impact on control [e.g., Price Waterhouse, 1981]. These elements can be classified as input mode and minicomputer hardware, physical environment, EDP staffing, application software, and systems software. Minicomputer-based processing is normally by on-line updating of single rather than batched controlled transactions [Douglas, 1982]. In such a processing environment, the effectiveness of the system of general controls will be greatly influenced by the control and security routines implemented as part of the operating system [AICPA, 1977]. Minicomputer operating systems (MOS) are regarded in the literature as being 'user friendly' [ICAEW, 1984 (b)], but incorporating fewer control and security routines than their mainframe counterparts relating to:

— Routines concerned with access to the computer system as a whole and to individual files [e.g., St. Clair, 1983];
— Routines concerned with recording details of transactions and individuals' processing action [e.g., Gottlieb, 1981]; and,
— Routines concerned with preventing and detecting unauthorised access or changes to application programs [Weber, 1982].

Objects

This paper details the results of an empirical examination of the Irish manufacturing sector, undertaken during 1984. Specifically, the study examines control and security routines implemented as part of the operating systems of minicomputers which process financial accounting applications, and demonstrates the potential internal control problems of minicomputer-based financial accounting applications arising from the

*The author is Head of the School of Accounting and Finance at the National Institute for Higher Education, Dublin, and currently Visiting Professor at the Fuqua School of Business, Duke University, North Carolina.

IBAR—Irish Business and Administrative Research, Volume 8, Part 2, 1986, pp 35-46.

empirical evidence regarding MOS. This will be achieved by comparison of the empirical evidence with those elements of internal control frameworks for computerised accounting application relating to operating system-based routines [e.g., AICPA, 1977 (b)].

Because the population frame had to be established directly (see Data Collection), the study had to be limited to one sector to keep it within reasonable bounds. The manufacturing sector was chosen because of its importance to the economic development of the country [NESC, 1982].

The Sampling Unit

Although attempts have been made to define "minicomputer" by reference to cost, processing capacity and performance [e.g., Leitch and Davis, 1983], there is no precise, generally accepted, definition of the term [Coopers and Lybrand, 1981]. This is mainly because attempts at classifying computers into 'mainframes', 'minis' and 'micros' are frustrated by the large number of machines with overlapping facilities [Stodel, 1980]. However, here is wide agreement that the minicomputer installation is characterised by small numbers of full-time EDP staff [BCS, 1981], and that multiuser, multitask processing[1], based on a single central processing unit, is the characteristic mode of processing of the minicomputer [Drew, 1980]. There is little further agreement about the characteristics of the minicomputer installation.

For the purpose of undertaking empirical research in this study, a minicomputer was defined as a computer which satisfied the following parameters:

P1, The computer was the only in-house computer on which the accounting system of the firm was processed;

P2, Was based on a single central processing unit and capable of supporting multiuser, multitask operations;

P3, Was not networked to another computer or computers; and,

P4, The EDP activities in the firm, in which the computer was located, were carried out by five or less full-time EDP staff.

The environment of single, stand-alone minicomputers is considerably different from that of multiple, stand-alone or networked minicomputers [McClure, 1980] and this study deals with the former case only. It is more correct to consider P1 and P3 as restrictions on the scope of the study which might well be required irrespective of the type of computer being studied. They should not be regarded as an intrinsic part of the definition of minicomputer except, perhaps, insofar as they exclude from the

definition certain computers which in themselves are not multiuser, multitask but which can be part of a larger system of networked computers which assumes those capabilities.

Data Collection

Because of the absence of reliable secondary sources, it was decided to establish the population frame directly. The number of manufacturing firms in Ireland is estimated to be 5,091 [CSO, 1981], of which only a small percentage use minicomputers. Therefore, investigation of all manufacturing firms was rejected because of the serious implications of non-response bias even if a high response rate could be achieved [Scott, 1961]. It was decied to establish the population by the iterative process which is summarised in Figure 1. A more detailed description of this proces is given in Walsh (1985).

Figure 2: Data Collection Steps

In step 1, a list of all makes of computers, marketed in Ireland together with their distributors was drafted from a wide range of sources (including catalogues of computer exhibitions, lists of members of trade associations, business and computer directories, magazines and newspapers) and verified by computer industry sources.

In step 2, as a 100% response was required, telephone interviews were conducted with the sales manager of the sole distributors of all makes of computer equipment marketed in Ireland. Where there was no sole distributor, all vendors were interviewed. From this process it was learned that, of the 91 makes of computer marketed for business data processing, 43 had models which fell within P2 above.

In step 3, distributors of the 43 makes were asked to supply a list of the firms who had been supplied with models within P2, except where the distributor was certain, based on records or other sources that a firm did not fall within P1, P3 or P4 or was not a manufacturing firm. After prolonged negotiation, all distributors agreed. Detailed guidance notes were prepared for vendors on the selection of firms (including action to be taken in the event of uncertainty).

In step 4, all 265 firms which were on the list were circulated with a mail questionnaire. 203 (76.6%) replied. T-tests, Standardised Proportion Difference tests and Chi Square tests, performed on the difference between means and proportions of replies received before and after a second reminder, showed no significant diference at the .05 level. As far as it is possible to judge from this approach (see Oppenheim, [1966, p. 24]), the results of the questionnaire were not materially biased because of non-response. 135 respondents actually fell within the definitions of 'Manufacturing Firm' and employed a 'Minicomputer' to process accounting applications (P1 to P4). It can be stated at the 95% confidence level that the population of such firms was between 168 and 187 [Cochran, 1977, pp. 9-62].

In step 5, a short article was included in "Irish Computer" magazine, designed to elicit replies from EDP managers in manufacturing firms with minicomputers who had not received a questionnaire. 14 replies were received but all fell outside the definitions of manufacturing firm and/or minicomputer at the cut-off date of the survey. This helps confirm the exhaustiveness of coverage of the target population.

Empirical evidence about MOS was collected by personal interviews, based on structured questionnaires, of EDP personnel in 124 of the 135 firms (91.9%) which were identified in step 5 of the process to establish the frame (see figure 1). This approach was used because it was possible that some of the personnel being questioned might not be highly trained or experienced in EDP [Best and Barrett, 1983]. This made it important that an interviewer be on hand to compensate. Nevertheless, care was taken not to bias replies. Interviews were carried out following the recommended procedures of Babbie (1973) and a glossary of unavoidable EDP terminology was prepared in advance to ensure consistency. The approach was pilot-tested in 10 firms which resulted in changes to the questionnaire and glossary.

The control and security routines examined were selected following a review of the literature which describes first, the perceived weaknesses of routines incorporated in MOS [e.g., Gottlieb, 1981] and second, the range of routines that are required to form part of an effective system of general controls [e.g., AICPA, 1979].

Empirical Evidence

Information regarding the implementation of routines concerned with access to the computer system as a whole and to individual files is presented in Tables 1 and 2 and discussed below: Of the 6 routines examined, identification numbers and passwords for entry to the computer system as a whole and file resource protection[2] were by far the most widely implemented; 97% of firms had implemented the former and just under 90% the latter. 30% of firms had implemented permitted menu display protection routines[3] and 25% routines for restriction of certain transactions to designated terminals. Virtually no firms had implemented label checking or automatic sign-off of terminals after a period of inactivity (3% and 2% respectively). On average, 3 of these 6 control routines were implemented and almost 90% of firms had a total of 2, 3 or 4 of them implemented. Less than 10% had a total of 5 routines implemented and only 1 firm (0.8%) had all routines.

Information regarding the implementation of routines concerned with recording details of transactions and individuals' processing actions is presented in Tables 3 and 4 Of the 10 routines examined, a group of 3 was considerably more widely implemented than the others. These were routines for recording the time of commencement and name of application programmes and utility programs used. Approximately

Table 1: *Routines Concerned With Access to the Computer System as Whole and to Individual Files — Extent of Implementation of Each Routine Examined*

Routines Implemented	Respondents n = 124		Population 95% Confidence Interval[1]
	No. of Firms	%	%
I.D. Number for Entry to System	120	96.8	95-98
Password for Entry to System	120	96.8	95-98
Permitted Menu Display	36	29.0	24-34
File Resource Protection	109	87.1	83-91
Magnetic Label Checking on Files	4	3.2	2- 5
Sign-Off of Terminals not in Use	3	2.4	1- 4
Restriction of Designated Transactions to Designated Terminals	32	28.5	21-31

[1] *The confidence limits are based on the normality approximation of the sampling distribution of the proportion with corrections for finite population (FPC) and continuity, except where the proportion is extremely small or extremely high ($p \leq .07$ or $\geq .93$) where the approximation is based on the Poisson distribution. As the population itself is estimated, the FPC is based on the higher limit for the population which is the most conservative approach* [Cochran, 1977, pp. 9-62].

Table 2: *Routines Concerned with Recording Details of Transactions and Individuals' Processing Actions — Total Number of Routines Implemented*

	Respondents: n = 124			Population
	No. of firms	%	Accum %	95% confidence Interval (%)
0	1	0.8	0.8	0- 2
1	2	2.4	3.2	1- 4
2	25	20.2	23.4	15-25
3	52	41.9	55.3	36-48
4	31	25.0	90.3	20-30
5	11	8.9	99.2	5-13
6	1	0.8	100.0	0- 2
	124	100.0		
Mean		3.2		
Median		3.0		
Standard Deviation		1.0		

Table 3: *Routines Concerned with Recording Details of Transactions and Individuals' Processing Actions — Extent of Implementation of Each Routine Examined*

	Respondents n = 124		Population 95% Confidence Interval
Routines Implemented	No. of Firms	%	%
Commence Time	107	86.3	82-91
Job Completion/Duration Time	101	81.5	14-23
Application Programs Used	93	75.0	70-80
Utility Programs Used	91	73.4	68-79
Records Modified	51	41.1	35-47
Alterations Made to Records	16	12.9	9-17
Identification of Performer	61	49.2	43-55
Unauthorised Access Attempts			
System	63	34.7	29-40
File	80	59.7	54-66
Program	21	16.9	12-22

Table 4: *Routines Concerned with Recording Details of Transactions and Individuals' Processing Actions — Total Number of Routines Implemented*

	Respondents: n = 124			Population
	No. of firms	%	Accum %	95% confidence Interval (%)
0	11	8.9	8.9	5-13
1	1	0.8	9.7	0- 2
2	9	7.3	17.0	4-11
3	9	7.3	24.3	4-11
4	28	22.6	46.9	18-28
5	16	12.9	59.8	9-17
6	8	6.5	66.1	3- 8
7	23	18.5	84.8	14-23
8	15	12.0	96.8	8-16
9	3	2.4	99.2	1- 4
10	1	0.8	100.0	0- 2
	124	100.0		
Mean		4.9		
Median		5.0		
Standard Deviation		2.5		

75%-85% of firms had implemented these routines. A second group of 4 routines was also implemented reasonably frequently. These were for recording of unauthorised attempts to access files (60% of firms implemented this routine), the identification of the performer of a job or transaction (49%), the records which were modified (41%) and unauthorised attempts to access the system as a whole (35%). The remaining group of 3 routines were more rarely implemented. These were for recording the alterations made to records (13%), unauthorised attempts to execute programs (17%) and the completion/duration time of a job or transaction (18%). On average, a total of 5 of these 10 logging routines was implemented. Almost 10% of firms had no routines implemented. Around two thirds of firms had between 2 and 7 of them implemented. Less than 6% had 9 or 10 routines implemented.

Information regarding the implementation of routines concerned with preventing and detecting unauthorised access or changes to application programmes is presented in Tables 5 and 6. The only 2 of these 5 routines which were implemented on any reasonable scale were routines for recording the date of the last change to a programme (38%) and the date of its creation (27%). The other routines were implemented in between 14% and 17% of firms. On average, only 1 routine was implemented.

Table 5: *Routines Concerned with Recording Details of Transactions and Individuals' Processing Actions — Total Number of Routines Implemented*

Routines Implemented	Respondents n = 124 No. of Firms	%	Population 95% Confidence Interval %
Program Designation as Test or Production	21	16.9	12-22
Program Creation Date	34	27.4	22-23
Date of Last Change to Program	47	37.9	32-44
Identity of Changer of Program	18	14.5	10-19
Date of Last Copy of Program	21	16.9	12-22

Table 6: *Routines Concerned with Preventing and Detecting Unauthorised Access or Changes to Application Programs — Total Number of Routines Implemented*

	Respondents: n = 124 No. of firms	%	Accum %	Population 95% confidence Interval (%)
0	73	58.9	58.9	53-65
1	3	2.4	61.3	1- 4
2	29	23.4	84.7	18-29
3	15	12.1	96.8	8-16
4	2	1.6	98.4	0- 3
5	2	1.6	100.0	0- 3
	124	100.0		
Mean		1.0		
Median		0.0		
Standard Deviation		1.3		

Almost 60% of firms had implemented no routines. 35% had implimented 2 or 3 routines and only 2 firms had implemented all 5 routines.

Potential Internal Control Problems in Minicomputer-Based Financial Accounting Applications arising from Empirical Evidence about Routines Concerned with Access to the Computer System as a whole and to Individual Files

The implications for internal control of the widespread non-implementation of 4 of these routines are:

(1) Permitted Menu Display: Non-implementation of this routine gives users and EDP staff an opportunity to "browse" with the computer system. Control is weakened by extensive knowledge of available programs among user and EDP staff.

(2) File Label Checking: Non-implementation of this routine increases the danger of wrong versions of files being processed. This could lead to inaccurate information being produced by financial accounting applications and to corruption and loss of data held as part of these appliations. Balancing procedures in purchased accounting appliation packages are often deficient [Warren, 1981] which increases these dangers.

(3) Automatic Sign-Off of Terminals After a Period of Inactivity: Non-implementation of this routine seriously undermines the effectiveness of ID/password protection and file resource protection against persons seeking to take unauthorised processing actions. It is not dificult to envisage such persons having the opportunity to execute transactions relating to financial accounting applications which they, themselves, are unauthorised to execute. They could do so by using terminals of staff with such authorisation which have been left unattended but "logged in".

(4) Restriction of Designated Functions to Designated Terminals: non-implementation of this routine also makes it easier for persons seeking to take unauthorised processing actions to do so. Any person who gains unauthorised knowledge of the password of another staff member will be able to execute any transaction, for which the other staff member is authorised, no matter how sensitive, from any terminal in the firm.

Potential Internal Control Problems in Minicomputer-Based Financial Accounting Applications Arising from Empirical Evidence about Routines Concerned with Recording Details of Transactions and Individuals' Processing Actions

The implications for control of the widespread non-implementation of many of these routines are:

(1) Unauthorised Attempts to (a) Access the System as a Whole, (b) Access Files, and (c) Execute Programs: To establish effective protection against persons seeking to take unauthorised processing actions, operating system based restrictions and controls must be supported by the production of reports on attempts to circumvent them. This allows management to investigate such attempts [Price Waterhouse, 1979]. Non-implementation of these routines eliminates an important element of the means of pinpointing staff who attempt unauthorised processing action. This pinpointing may also help bring to light successful circum-

vention. Therefore, important vehicles for the prevention, detection and correction of unauthorised interference with data held as part of financial accounting applications are lost, as is the deterrent value of the activity on the potential perpetrator of fradulent processing.

(2) The identification of the Performer of a Job or Transaction; Non-implementation of this routine in a multiuser, Multitask processing environment has far-reaching consequences for control. It makes it almost impossible to establish full individual accountability for processing actions. Therefore, the source of erroneous, irregular and unauthorised transactions may be untraceable. Knowledge of this fact may make staff less careful about their legitimate processing transactions and encourage those tempted to preparate unauthorised transactions by reducing the danger of their detection. This danger may be offset to some extent by the smaller number of terminals and users in minicomputer installations [Shearon, Butler and Benjamin, 1980].

(3) (a) Records Modified and (b) Alterations Made to Each Record in a Job or Transaction: Non-implementation of these routines makes it impossible to operate automatic, operating system-generated recovery of data-files, in the event of computer failure. When taken in conjunction with weaknesses in transaction logging in purchased accounting application packages used on minicomputers [Warren, 1981], the danger of loss of data in minicomputer-based financial accounting applications must be considered serious. Non-implementation of these routines makes it impossible to use operating system-generated logs in the provision of audit trail.

(4) The Completion or Duration Time of a Job or Transaction: The comparing by management reports of actual processing activity, as logged by operating system, against planned activity and schedules is a further important element in the detection of unauthorised processing [Beck, 1982]. Absence of information on the length of time spent on jobs or transactions must weaken considerably the value of the reports.

Potential Internal Control Problems in Minicomputer-Based Financial Accounting Applications Arising from Empirical Evidence about Routines Concerned with Preventing and Detecting Unauthorised access or changes to Application Programmes

Where the firm uses in-house developed or modified financial accounting applications, the widespread non-implementation of all of these routines makes it more difficult for management to detect unauthorised changes

to financial accounting application software which compounds the problems of concentration of EDP duties associated with minicomputer installation [Porter and Perry, 1984]. The effects of this control weakness are, however, offset by the widespread use of application packages, for which the source code is unlikely to be available within the firm [AICPA, 1981,]. The non-implementation of routines which record whether application programs are test or production status may mean that this distinction does not exist at an operational level. If this is the case, it again increases the danger of unauthorised interference with financial accounting application programs in firms with the relevant source code.

Summary and Conclusions

Only about half the operating systems-based routines examined which are concerned with (a) access to the computer system as a whole and to individual files, and, (b) recording details of transactions and individuals' processing actions, are widely implemented in manufacturing firms with minicomputer-based financial accounting applications. Routines concerned with preventing and detecting unauthorised access or changes to application programs are implemented very infrequently indeed. As a result, there is unlikely to be an adequate framework for the prevention of unauthorised processing relating to financial accounting applications through terminals, nor sufficient data to detect that such unauthorised processing has taken place and to pinpoint the prepetrator.

In the event of computer failure, automatic recovery of datafiles, will not normally be possible and operating system generated logs cannot be used to provide an audit trail. There is consequent serious danger of loss of accounting data. There is increased danger of processing wrong versions of accounting datafiles and, where the source versions of accounting application programs are available, they are very vulnerable to unauthorised interference. In the majority of cases in the manufacturing sector, an auditor of minicomputer-based financial accounting applications is unlikely to find the conditions which permit reduction in audit testing by placing reliance on general controls (for a discussion of these conditions, see AICPA(1983)). This is because of the nature and range of the likely problems with general controls which emerged from this study.

NOTES

1. Multiuser, multitask processing allows a number of users to carry out different processing tasks on the computer at the same time.
2. The file resource protection routines allow the specification of the users with authority to read, modify or execute the contents of files and/or libraries of files and the automatic limiting of the ability to carry out these functions to those so specified.
3. Permitted menu display protection routines allow the display to each user of only those transactions which he or she is authorised to perform. This display is in the form of a list or "menu".

REFERENCES

American Institute of Certified Public Accountants, 1977(a), The Auditor's Study and evaluation of Internal Controls in EDP Systems. New York.

American Institute of Certified Public Accountants, 1977(b). *Management, Control and Audit of Advanced EDP Systems.* New York.

American Institute of Certified Public Accountants, 1979. *Controls Over Using and Changing Computer Programs.* New York.

American Institute of Certified Public Accountants, 1981. *Audit and Control Considerations in a Minicomputer or Small Business Computer Environment.* New York.

American Institute of Certified Public Accountants, 1983. *The Effects of Computer Processing on the Examination of Financial Statements.* New York.

Babbie, R.E., 1973. *Survey Research Methods.* Belmont, Cal.: Wadsworth Publishing.

Beck, M., 1982. "How to Get Control in Real-Time Interactive Systems", *Accountancy,* May 1982, pp. 126-131.

Best, P. and Barrett, P., 1983 *Auditing Computer Based Accounting Systems.* Sydney: Prentice-Hall.

British Computer Society, 1981. *Control and Audit of Minicomputer Systems.* London: Hayden.

Central Statistics Office, 1981. *Census of Industrial Production.* Dublin.

Cochran, W.G., 1977. *Sampling Techniques.* New York: Wiley.

Coopers and Lybrand, 1981. *Manual of Auditing.* London: Gee and Co.

Douglas, I.J., 1982. *Audit and Control of Mini- and Microcomputers.* Manchester: National Computing Centre.

Drew, J., 1980. "Accounting for Internal Control in the Age of the Small Business Computer", *Accountancy Age,* 4 April 1980, pp. 26-27.

Gottlieb, M., 1981. "Audit Concerns about Minicomputers", *Edpacs,* October 1981, pp. 12-15.

Institute of Chartered Accountants in England and Wales, 1984(a). *Auditing Guideline — Auditing in a Computer Environment.* London.

Institute of Chartered Accountants in England and Wales, 1984(b). *Computer Security.* London.

Leitch, R.A. and Davis, K.R., 1983 *Accounting Information Systems.* Englewood Cliffs, NJ: Prentice-Hall.

McClure, D., 1980. "Network Security and control in Distributed Data Processing", *The EDP Auditor,* Wintor 1980, pp. 67-70.

National Economic and Social Council, 1982. *A Review of Industrial Policy.* Dublin.

Oppenheim, A.N., 1966. *Questionnaire Design and Attitude Measurement.* London, Heinnemann.

Porter, W.T. and Perry, W.E., 1984. *EDP Controls and Auditing.* Boston: Kent Publishing Co.

Price Waterhouse, 1979. *Accounting Controls in a Minicomputer Environment.* New York.

Scott, C., 1961. "Research on Mail Surveys", *Journal of the Royal Statistical Society,* 2, p. 147.

Shearon, W., Butler, C. and Benjamin, J., 1980. "Audit Aspects of Small Computer Systems", *The CPA Journal,* August 1980, pp. 17-21.

St. Clair, L., 1983. "Security for Small Computer Systems", *Edpacs,* November 1983, pp. 1-10.

Stodel, H., 1980. "The Small Business Computer and the Accountant", *South African Chartered Accountant,* August 1980, pp. 341, 342.

Walsh, J.A., 1985. *Control in Minicomputer-Based Financial Accounting Applications* Ph.D. Thesis, City University, London.

Warren, A., 1981. "Controls and the Minicomputer: An Auditor's View", *Accountancy,* December 1981, pp. 119-120.

Weber, R., 1982. *EDP Auditing: Conceptual Foundations and Practice.* New York: McGraw-Hill.