

An Analysis Of Controls And Perceived End-User Productivity Between Accounting And Non-Accounting Majors In A Microcomputer Environment

Raymond Landry Jr.(rlandry@gsvms2.cc.gasou.edu), Georgia Southern University

Abstract

This study demonstrates that perceived PC use under a variety of control procedures varies widely among accounting, management, and computer science majors sampled in this study. In addition, a large percentage of all respondents believed that control procedures tended to discourage PC use. Of the significant differences noted, most occurred between the computer science majors and the other two groups of students where the computer science majors perceived more strongly that the control procedures tended to discourage their PC use.

Introduction

For accounting majors, discussion of internal controls is a very important concept in an accounting information systems course whereby the emphasis is on protecting company assets and insuring the integrity of the financial statements. While non-accounting majors may learn about controls in a management information system or a system analysis and design course, their viewpoint may be entirely different such as emphasizing cost-effectiveness and efficiencies. When these students graduate and become the auditors, managers, and systems personnel who make decisions

regarding controls, will their schooling cause a different perception of the role of internal controls in an organization? With the increase of end-user computing¹ in many companies, auditors want to insure that any access to financial statement data is properly secured, management is looking for increased productivity as end-users make greater use of their microcomputers (PC's) and software while systems people want to make sure all computer system are running smoothly with very little downtime.

However, consider the following situa-

tions that might arise in any PC environment as shown in Table 1. Whether these situations are acceptable practices, mildly tolerated, or not tolerated at all, may depend on individuals within the company. While some individuals may tolerate these activities, others may have a different view. The real question is "why do these situations occur?" Many reasons might be cited such as: "...it's not worth the effort...", "...costs too much...", "...nobody is going to steal anything...", or "...we are all one big happy family, nothing could go wrong". It might be proposed that how one perceives a control procedure to impact an end-user's productivity² might be a contributing factor in deciding whether or not to implement a specific control procedure. Raval [1990] argued that focusing on user-friendly (i.e. promoting system usage) procedures did not always support control objectives.

It is also quite possible the more PC control procedures involved, the less productive an employee might be in a PC-based environment believing the control to be a hindrance rather than a help. In order to overcome this, Frese [1987] suggests that "having control over conditions and one's actions leads to positive motivational and cognitive consequences". However, many still view controls in general as anything but insuring productivity. Czarnecki [1982] reported that managers viewed controls as a low priority item while employees viewed controls as "frustrating and cumbersome". Many

other issues might also be raised such as: (1) Will controls be compromised in a PC environment in order to promote user productivity? (2) How will actual conflicts concerning control procedures be remedied between auditors, managers, or systems analysts? (3) Should management let up on control procedures in order to encourage more PC use? and (4) How will end-users react under too many or too few controls?

The answer to these questions may lie in one's understanding of control procedures and its impact on perceived productivity. Students majoring in accounting will first be exposed to internal controls in the accounting information systems class and then repeated in the auditing class where the emphasis is on insuring the reliability of the financial statements. Non-accounting majors such as management and computer science are likely to find a discussion of control issues in a management information systems or a system design course. When it comes to controls in a PC environment, will they have a different perception of the role internal controls and will this be affected by perceived productivity of the end-users?

Purpose For The Study

The purpose for this study is to examine the perceptions concerning controls and procedures in a PC environment among accounting, management, and computer science majors who

Situation	Control Procedure
Passwords on "stick-um" notes are pasted to many PC monitors or found in the top desk drawer of employees' desks.	Passwords should be memorized and not written down for unauthorized use.
End-users are building untested and undocumented models for data analysis which are passed around to other employees for their use.	All end-user built models are thoroughly tested and documented.
Unauthorized gaming or shareware programs are found on company PC's.	No software should be installed on any PC unless it has been okayed by management and examined by virus detection software.
Employees are "surfing" the internet on company time.	No random searches on the internet without a deliberate goal or objective.

eventually will become the auditors, managers and systems personnel of the future. Insuring a proper balance between controls and maintaining a highly efficient and productive work environment is a very difficult task. As Yarberr and Summers [1994] explain, "Despite the many advantages of small computer technology and distributed systems, the control systems surrounding newer IT systems are immature." However, "...it is ultimately the prevailing control attitude, not the technology...". While controlling every threat to PC security is not possible or cost effective, emphasis needs to be placed on those violations that are probable (Levi [1993]). However, if differing views exist among the various professionals within an organization concerning where control emphasis needs to be placed, conflicts may arise that might allow risky situations to thrive which eventually will have a detrimental effect on the organization.

Results of this study for accounting information systems' faculty will be helpful as students learn about internal controls and that an accounting view of control procedures may be different from those of a management view or system design perspective. Although accountants will be very ambitious to protect the integrity of the financial statements, if the financial statements are output from PC-based systems, much interactivity will occur between accountants, managers, and systems designers concerning appropriate controls and procedures.

Previous Research

Internal Control Evaluations

Previous studies examining internal control evaluations began with auditor judgments measuring consensus and consistency. Later, comparisons of judgments between auditors verses other professionals, auditors verses student surrogates, and the use of more sophisticated manual environments as well as various components of the audit process were also examined. In addition, experience and firm differences were also studied as possible explanatory variables for any consensus differences. (See

Ashton [1974], Reckers and Taylor [1979], Ashton and Brown [1980], Gaumnitz et.al. [1982], Hamilton and Wright [1982], and Haskins [1987].) While there appears to be a wide range of levels of consensus concerning auditor judgments, most of the researchers concluded that there is agreement among auditors concerning internal control evaluations.

Weber [1980] expanded previous research in several ways. He examined auditor consensus using internal controls as part of electronic data processing (EDP) situations and not primarily manual environments. In addition, he compared internal control judgments among and between external auditors, internal auditors, and accounting students.

Later research (Bailey [1990]) concerning internal control judgments between auditors and other accounting professionals (certified internal auditors) found some agreement between the two groups. However, the internal auditors appeared to have a much stricter view of internal controls than the external auditors.

The only study examining the judgments of auditors and non-accounting systems professionals concerning internal controls was conducted by Grabski et.al. [1987]. The results of this study were mixed. While no significant differences were found between the groups in general, small differences were found in each groups recommendations concerning specific EDP general and application controls.

This study extends the previous research three ways. First, by sampling students who will become the future auditors, managers, and systems analysts, any differences will be identified before these differences become a risky situation in the business world. Secondly, this study looks at PC-based controls and procedures that were either not in existence or relatively new at the time these previous studies were conducted. Thirdly, the effect of control procedures as it relates to perceived user productivity is examined as a possible contributing factor to differences in control viewpoints.

Research Design

Sample

Data from junior and senior level college students from two different universities located in the southeast was collected over several different time periods.³ Respondents in this study included 101 students majoring in accounting, 92 management majors, and 81 students majoring in computer science.

Survey Instrument

The survey instrument included demographic questions such as GPA, age, gender, major, and years experience with PC's in school and work. While all respondents were instructed to read the directions, they were verbally informed that the responses were based on their perception of how end-users would react given the particular control procedure. In addition, the accounting majors were verbally instructed to view this questionnaire as if they were auditors, management majors as if they were managers, and computer science majors were instructed to answer from the viewpoint of system analysts. The questionnaire required the students to respond to twenty-two control procedures⁴ (found in Table 2) and rate its effect on their perceived PC use based on a five-point Likert scale. The scale ranged from "highly encourage", "slightly encourage", "no effect", "slightly discourage", and "highly discourage".

Hypothesis

In the major hypothesis, how each group perceived the control environment and its effect on PC use was analyzed. Therefore, the following hypothesis (in the alternate form) was tested:

H_a: There is a difference in the perception of end-user PC usage under various control procedures between accounting majors, management majors, and computer science majors.

In addition to examining the first hypothesis, the percentage of students who viewed

these controls as inhibiting an end users PC usage was also of interest. It is theorized that any control procedure which is perceived as inhibiting PC use would result in an individual either ignoring the control procedure or opting to avoid using the PC which may cause a decrease in productivity.

Statistical Tests

Since the responses to the instrument were categorical rather than continuous, statistical analysis was done using the chi-square test of homogeneity. With this test, the null hypothesis is examined to see if the populations are homogeneous concerning the proportion of their responses falling under the various levels of the likert scale.

Analysis Of Results

Sample Demographics

The students sampled in this study had the following characteristics. The majority of accounting students were female, 21-22 years old with a grade point average between 3.00 and 3.25. Accounting majors also claimed to have at least 3 years experience working with PC's. Management majors were male dominated, had GPA's averaging 2.75-3.00 and indicated on average less than 2 years experience working with PC's. Eighteen to twenty year old males dominated the computer science majors who had GPA's and PC years of experience similar to the accounting majors.

Analysis of Control Procedures and Related PC Use

The control procedures, the frequency distributions of responses,⁵ and the level of significance (if statistically significant) are shown in Figures 1-22 found in the appendix. As seen from these figures, a wide range of perception of encouraged or discouraged PC use exists not only between the majors but also among the majors. Control procedures 1, 3, 6, 8, 13, 14, 17, 19, 20, and 22 were found to have significant

Table 2
PC Controls and Procedures

<ol style="list-style-type: none"> 1 In order to use a PC, a user id and password must be entered. 2 Every user's password is changed monthly to prevent unauthorized password use. 3 System documentation is highly detailed and written in a very technical manner. 4 Purchased software from outside the company is not allowed on any PC. 5 Much of the company software is menu driven with help facilities online. 6 Smoking, eating, and drinking are not permitted while working on any PC. 7 No one is permitted to use the company's PC's after normal business hours. 8 There is always a supervisor or system support personnel around to monitor and help when PC problems occur. 9 All floppy disks must be examined on a regular basis for viruses. 10 No data or program disks may be copied or removed from company premises. 11 No personal use of any PC is allowed. 12 Program and data disks not being used are stored in a locked cabinet and controlled by a software manager. 13 Any user developed model is not allowed to be used by other employees until fully tested and documented. 14 Uploading or downloading data between a mainframe and PC requires a supervisor's approval. 15 Every user must undergo a training session before being allowed on company PC's. 16 A software manager needs to be appointed to oversee all company software purchases, registrations, and licensing agreements. 17 All company employees need to be familiar with a software code of ethics. 18 All company employees need to be familiar with software licensing agreements. 19 The company should audit all PC's on a periodic and surprise basis for illegal and unlicensed software. 20 Access to a company's program and data files should be on a need-to-know basis. 21 Random internet surfing is not allowed during company time. 22 Downloading shareware or freeware from the internet requires supervisor approval and must be scanned with virus detection software.

differences and are discussed below.

CONTROL 1 The significant differences ($\chi^2 = 16.36, p < .01$) in perceived user productivity appear to occur between the computer science students and the other two majors. From Figure 1, it can be seen that accounting and management students were not as encouraged by this control procedure as were the computer science students. Perhaps the computer science students fully understood the importance of this control in order to stop any unauthorized accesses where the accounting and management students felt that having to enter an id and password only slowed productivity down. Also contributing to the differences was the higher percentage of both accounting and management students responding that this procedure discouraged their PC usage.

CONTROL 3 As expected, significant differences ($\chi^2 = 12.85, p < .05$) for this procedure were caused by the computer science majors. Compared to the accounting and management majors (in Figure 3) who indicated they perceived PC use to be strongly discouraged, the computer science majors indicated they perceived PC use would be more encouraged when detailed documentation was provided. From a practical standpoint, software packages often contain documentation that only a system developer or programmer is able to understand while auditors and managers might have to rely on others or find themselves in the local bookstore buying paperback books that explain the software in simpler terms. It is interesting to note the frequency distribution found for this question among the different majors. While 44% and 50%

of the accounting and management majors respectively were encouraged, 47% and 43% (respectively) indicated they would be discouraged if the documentation was too highly detailed and technical. The computer science majors as anticipated were more encouraged (69%) than discouraged (26%).

CONTROL 6 Significant differences in perceptions of PC use ($\chi^2 = 9.93, p < .05$) due to this control procedure were found between the different majors primarily based on the accounting majors' large percentage of encouraged responses. Initially, this control was theorized to be an inconvenience and thus the majority of respondents would have indicated that it discouraged PC use. While management and computer science majors indicated that a large percentage were encouraged by the control procedure of not allowing eating, drinking and smoking as shown in Figure 6, there was also a large percentage of computer science majors who indicated they perceived PC use would be highly diminished if users were required to work under this rule.

CONTROL 8 Having a supervisor or information support people around to answer questions or resolve problems for management and end users would certainly encourage PC use as indicated in the Figure 8. However, significant differences ($\chi^2 = 19.00, p < .01$) were found between accounting and computer science majors, and between management and computer science majors. Compared to accounting and management majors, the computer science majors perceived end-users would not be as encouraged. It would seem that having help available should encourage PC use, however, perhaps the computer science majors thought themselves to be the ones providing the help, thus their own work would not be getting done.

CONTROL 13 Significant differences ($\chi^2 = 8.16, p < .10$) were found between accounting and management majors, and accounting and computer science majors. While both management and computer science majors indicated they perceived users to be encouraged by this control, accounting majors were not as encouraged as

shown in Figure 13. This result was very surprising. Testing and documentation are taught as very important controls to accounting majors and as such should have indicated that this control should have encouraged PC use. Results also show that accounting majors felt users would be more discouraged to use the PC under this control procedure than any of the other majors. The significance of this control procedure is very important. In today's highly dynamic PC environments, many end users are continuously building their own models to process company data such as spreadsheet and database models. These user-developed models tend to be untested (i.e., "if it works, it must be error free" syndrome) and undocumented except for the rules and procedures the user who developed this model might remember.

CONTROL 14 The transferring of data between the mainframe and network (via PC) needs to be controlled. As shown in Figure 14, both accounting and management majors were more similar in their perceptions regarding this control procedure than the computer science majors. Highly significant differences ($\chi^2 = 41.24, p < .01$) were found for this procedure caused by the computer science major's large percentage of perceived discouraged use. This view may be explained by the fact that the computer science majors may have a greater need to be able to work between the mainframe and network. Thus every time data is uploaded or downloaded between the mainframe and network, having to seek supervisor approval may discourage their use of the system.

CONTROL 17 The introduction of ethics in the business schools and computer science curriculums is fairly new. While there is much controversy over the fact of whether or not ethics can be taught, students must still have some concept of what is considered ethical verses unethical. A software (or computer) code of ethics should be an integral part of every company's organizational policies. Although there were large majorities of all majors indicating they believed that PC use might be strongly encouraged by this procedure as shown in Figure 17, significant dif-

ferences were found ($\chi^2 = 8.13, p < .10$) due to the higher percentage of discouraged use indicated by the computer science majors. These differences between the respondents will probably be reduced in the future as the study of ethical issues is incorporated into the academic curriculum.

CONTROL 19 Periodic and surprise audits of computer and software systems is a very important control procedure. Audits are important to a company in detecting unlicensed software, shareware brought in and loaded on company computers, undocumented computer models or programs, etc. Therefore, audits serve a very useful function. As such, PC use should be encouraged by this procedure. While all three majors indicated that they believed that this procedure would encourage use, a significant difference was found ($\chi^2 = 10.74, p < .05$) due to the larger percentage of computer science majors (see in Figure 19) who indicated PC use would probably be discouraged by this procedure.

CONTROL 20 Significant differences ($\chi^2 = 7.83, p < .10$) were the result of accounting majors indicating that PC use would be discouraged if access to a company's programs and data files were on a need-to-use basis. Management and computer science majors were similar in their perceptions with similar percentages between those encouraged and discouraged by this control as shown in Figure 20.

CONTROL 22 The downloading of software off the internet is a common activity in today's organizations. Accounting majors perceived that PC use would be encouraged among end-users probably because of the safeguards virus detection software can give. However, significant differences were found ($\chi^2 = 11.04, p < .05$) due to management and computer science majors not being as positive. These majors perceived that PC use would be discouraged if users were required to comply with this control procedure.

Control Procedures and Discouraged PC Usage

The final part of this study surveyed the

relationship between the control procedures and the respondents' views concerning whether these controls in general appear to encourage or discourage PC use. It was asserted at the beginning of this paper that controls may be negatively associated with PC use. As shown in Table 3, many of the control procedures as viewed through the eyes of the students, were perceived to discourage PC use. For the accounting majors, 33% of the sample indicated that they perceived the control procedure to discourage end-user computing. Computer science majors indicated a slightly larger percentage, 34%, while management majors perceived end-user productivity would be discouraged by 31%. These survey results are quite surprising. Over one-third of the accounting majors indicated they believed that PC control procedures would discourage PC use. Internal controls in accounting systems are very important, but do students understand that these controls are controlling people's jobs or functions? It is understandable that no matter how well controlled a particular situation or application is, if user's revolt or productivity diminishes due to these control procedures, there will be problems to deal with.

Future Research

As in all studies of this nature, certain assumptions and limitations must be addressed. Although considered acceptable surrogates, students were used in this study whereas actual auditors, managers, and system analysts sampled regionally or nationally may have been more suitable. In addition, a questionnaire was used with a listing of control procedures that were viewed individually rather than looking at the whole business control framework. Future research may investigate these controls under more sophisticated conditions using a live business environment and career professionals.


Conclusions

This study has demonstrated that perceived PC use under a variety of control procedures varied widely between accounting, management, and computer science majors sampled

Table 3			
PC Controls and Procedures and Perceived Discouraged Use			
	Accting	Mgmt	CS
1 In order to use a PC, a user id and password must be entered.	22%	28%	5%
2 Every user's password is changed monthly to prevent unauthorized password use.	41%	35%	38%
3 System documentation is highly detailed and written in a very technical manner.	47%	43%	26%
4 Purchased software from outside the company is not allowed on any PC.	61%	59%	59%
5 Much of the company software is menu driven with help facilities online.	8%	4%	9%
6 Smoking, eating, and drinking are not permitted while working on any PC.	10%	20%	22%
7 No one is permitted to use the company's PC's after normal business hours.	73%	62%	79%
8 There is always a supervisor or system support personnel around to monitor and help when PC problems occur.	15%	9%	33%
9 All floppy disks must be examined on a regular basis for viruses.	9%	9%	9%
10 No data or program disks may be copied or removed from company premises.	35%	38%	30%
11 No personal use of any PC is allowed.	54%	59%	53%
12 Program and data disks not being used are stored in a locked cabinet and controlled by a software manager.	53%	54%	63%
13 Any user developed model is not allowed to be used by other employees until fully tested and documented.	41%	26%	31%
14 Uploading or downloading data between a mainframe and PC requires a supervisor's approval.	40%	22%	65%
15 Every user must undergo a training session before being allowed on company PC's.	4%	4%	4%
16 A software manager needs to be appointed to oversee all company software purchases, registrations, and licensing agreements.	17%	21%	17%
17 All company employees need to be familiar with a software code of ethics.	10%	4%	15%
18 All company employees need to be familiar with software licensing agreements.	7%	4%	7%
19 The company should audit all PC's on a periodic and surprise basis for illegal and unlicensed software.	9%	4%	19%
20 Access to a company's program and data files should be on a need-to-know basis.	34%	18%	23%
21 Random internet surfing is not allowed during company time.	83%	84%	73%
22 Downloading shareware or freeware from the internet requires supervisor approval and must be scanned with virus detection software.	48%	68%	67%
Average % of perceived discouraged use	33%	31%	34%

in this study. In addition, a large percentage of all respondents believed that control procedures tended to discourage PC use. Of the significant differences noted, most occurred between the computer science majors and the other two groups of students where the computer science majors perceived more strongly that the control procedures tended to discourage their PC use. The differences found between these future system analysts and future auditors in this study was expected and hoped for. As Grabski et. al. [1987] have suggested:

If auditors were shown to have superior skills, say in the identification of internal control weaknesses, then improved controls could result from auditor involvement in system design. Alternatively, if no difference in control identification exists between auditors and systems analysts, then it could be argued that systems analysts have the necessary skills to design a well controlled system.

Control procedures are not meant to discourage legitimate use. For the most part, controls at best offer intangible benefits that are rarely appreciated until a situation arises when an unwanted event is thwarted, or where damage is kept to a minimum due to control procedures. Encouraging PC use among a company's employees and being able to control the environment is a task that will require cooperation among all those involved. Where differences exist, the solution may lie in better education and open communication between auditors, managers, and system designers such that all understand the purpose and use for certain control procedures. 

Notes

1. End-user computing is defined as the hands-on use of computer technology whereby employees other than data processing professionals access company data for business purposes (Johnson and Raymond [1994]).
2. For this study, productivity is simply viewed as promoting the use of one's PC

verses attempting to accomplish a task without using a PC. For a more detailed discussion from the end-user's perspective see Davis [1989].

3. Chi-square tests of homogeneity were conducted for differences between students in the two universities as well as the differing time periods. Two of the twenty-two control situations were found to be significantly different by students at one university while not significant at the other. These differences however, should not materially affect the conclusions reached in this paper. No significant differences were found between student data collected over the different time periods.
4. Control procedures were gathered from many sources. Initially, there were thirty-three controls. Some of these procedures were perceived as redundant or outdated by a test group of students in a graduate EDP Auditing course who evaluated the original instrument thus reducing it to twenty-two control procedures.
5. Although the data was collected using a five-point likert scale, this data was collapsed (due to missing values in cells) for statistical purposes into three categories of encouraged, no effect, or discouraged use.

References

1. Ashton, R.H., "An Experimental Study of Internal Control Judgments," *Journal of Accounting Research* (Spring 1974), p. 143-157.
2. Ashton, R.H. and P.R. Brown, "Descriptive Modeling of Auditors' Internal Control Judgments: Replication and Extension," *Journal of Accounting Research* (Spring 1980), p. 269-277.
3. Bailey, C.D., "CIA's and CPA's: Do They Agree on Internal Accounting Controls?" *Internal Auditor* (February 1990), p. 46-49.
4. Czarnecki, G.M., "Internal Controls: Executive Management Responsibility," *The Magazine of Bank Administration*, (June 1982), p. 20-24.

5. Davis, F.G., "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, (September 1989), p. 319-339.
6. Frese, M., "A Theory of Control and Complexity: Implications for Software Design and Integration of Computer Systems into the Workplace," *Psychological Issues of Human Computer Interaction in the Work Place*, (1989), p. 313-337.
7. Gaumnitz, B.R., T.R. Nunamaker, J.J. Surdick, and M.F. Thomas, "Auditor Consensus in Internal Control Evaluation and Audit Program Planning," *Journal of Accounting Research* (Autumn 1982), p. 745-755.
8. Grabski, S.V., J.H. Reneau, and S.G. West, "A Comparison of Judgement, Skills, and Prompting Effects Between Auditors and Systems Analysts," *MIS Quarterly* (June 1987), p. 151-161.
9. Hamilton, R.E. and W.F. Wright, "Internal Control Judgments and Effects of Experience: Replications and Extensions," *Journal of Accounting Research* (Autumn 1982), p. 756-765.
10. Haskins, M.E., "Client Control Environments: An Examination of Auditors' Perceptions," *The Accounting Review* (July 1987), p. 542-563.
11. Johnson, S.J. and M.J. Raymond, "Controlling End-User Computing," *Management Accounting* (September 1994), p. 66-69.
12. Levi, P., "Your PC's are More Vulnerable Than You Think," *Chief Information Officer Journal* (March/April 1993), p. 11-13.
13. Raval, V., "Do User-Friendly Systems Enhance Control Objectives?" *Journal of Accounting and EDP*, (Spring 1990), p. 24-27.
14. Reckers, P.M.J. and M.E. Taylor, "Consistency in Auditors' Evaluations of Internal Accounting Controls," *Journal of Accounting, Auditing, and Finance* (Fall 1979), p. 42-44.
15. Weber, R., "Some Characteristics of the Free Recall of Computer Controls by EDP Auditors," *Journal of Accounting Research* (Spring 1980), p. 214-241.
16. Yarberry, W.A. and G.E. Sumners, "The Evolution of Information Technology Controls," *Internal Auditing* (Summer 1994), p. 32-39.

Appendix I Computer Usage Survey

Major: <input type="checkbox"/> Accounting	Gender: <input type="checkbox"/> Female	GPA: <input type="checkbox"/> less than 2.0	Computer <input type="checkbox"/> home
<input type="checkbox"/> Computer Science	<input type="checkbox"/> Male	<input type="checkbox"/> 2.0 - 2.25	Experience: <input type="checkbox"/> less than 2 years
<input type="checkbox"/> Management		<input type="checkbox"/> 2.26 - 2.50	<input type="checkbox"/> 3 years
<input type="checkbox"/> Other _____	Age: <input type="checkbox"/> 18-20	<input type="checkbox"/> 2.51 - 2.75	<input type="checkbox"/> greater than 3 years
	<input type="checkbox"/> 21-22	<input type="checkbox"/> 2.76 - 3.00	
	<input type="checkbox"/> 23-25	<input type="checkbox"/> 3.01 - 3.25	school / work
	<input type="checkbox"/> Over 25	<input type="checkbox"/> 3.26 - 3.50	<input type="checkbox"/> less than 2 years
		<input type="checkbox"/> 3.51 - 3.75	<input type="checkbox"/> 3 years
		<input type="checkbox"/> 3.76 - 4.00	<input type="checkbox"/> greater than 3 years

DIRECTIONS: Please respond to the following control procedures and indicate how you perceive an end-user would react regarding the use of their PC.

	Highly Encourage	Encourage	Neutral	Discourage	Highly Discourage
	-----	-----	-----	-----	-----
1 In order to use a PC, a user id and password must be entered.	[]	[]	[]	[]	[]
2 Every user's password is changed monthly to prevent unauthorized password use	[]	[]	[]	[]	[]
3 System documentation is highly detailed and written in a very technical manner.	[]	[]	[]	[]	[]
4 Public domain software from outside the company is not allowed on any PC.	[]	[]	[]	[]	[]
5 Much of the company software is menu driven with help facilities online.	[]	[]	[]	[]	[]
6 Smoking, eating, and drinking are not permitted while working on any PC.	[]	[]	[]	[]	[]
7 No one is permitted to use the company's PC's after normal business hours.	[]	[]	[]	[]	[]
8 There is always a supervisor or system support personnel around to monitor and help when PC problems occur.	[]	[]	[]	[]	[]
9 All floppy disks must be examined on a regular basis for viruses.	[]	[]	[]	[]	[]
10 No data or program disks may be copied or removed from company premises.	[]	[]	[]	[]	[]
11 No personal use of any PC is allowed.	[]	[]	[]	[]	[]
12 Program and data disks not being used are stored in a locked cabinet and controlled by a software manager.	[]	[]	[]	[]	[]
13 Any user developed model is not allowed to be used by other employees until fully tested and documented.	[]	[]	[]	[]	[]
14 Uploading or downloading data between a mainframe and PC requires a supervisor's approval.	[]	[]	[]	[]	[]
15 Every user must undergo a training session before being allowed on company PC'	[]	[]	[]	[]	[]
16 A software manager needs to be appointed to oversee all company software purchases, registrations, and licensing agreements.	[]	[]	[]	[]	[]
17 All company employees need to be familiar with a software code of ethics.	[]	[]	[]	[]	[]
18 All company employees need to be familiar with software licensing agreements.	[]	[]	[]	[]	[]
19 The company should audit all PC's on a periodic and surprise basis for illegal and unlicensed software.	[]	[]	[]	[]	[]
20 Access to a company's program and data files should be on a need-to-know basis	[]	[]	[]	[]	[]
21 Random internet surfing is not allowed during company time.	[]	[]	[]	[]	[]
22 Downloading shareware or freeware from the internet requires supervisor approval and must be scanned with virus detection software.	[]	[]	[]	[]	[]

Figure 1

1. In order to use a PC, a user id and password must be entered.

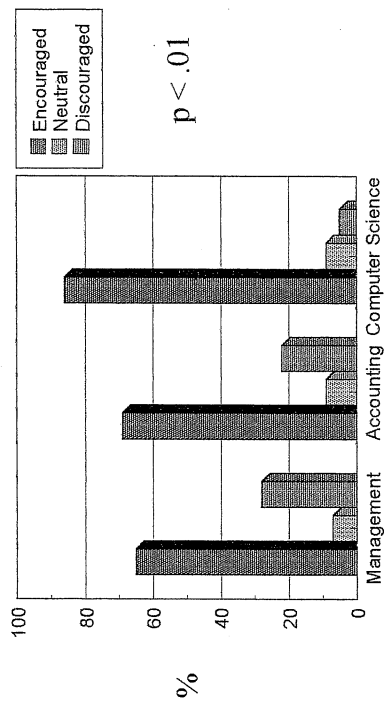


Figure 2

2. Every user's password is changed monthly to prevent unauthorized password use.

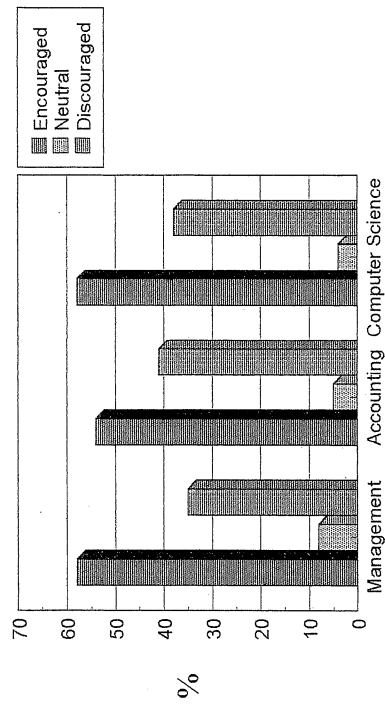


Figure 3

3. System documentation is highly detailed and written in a very technical manner.

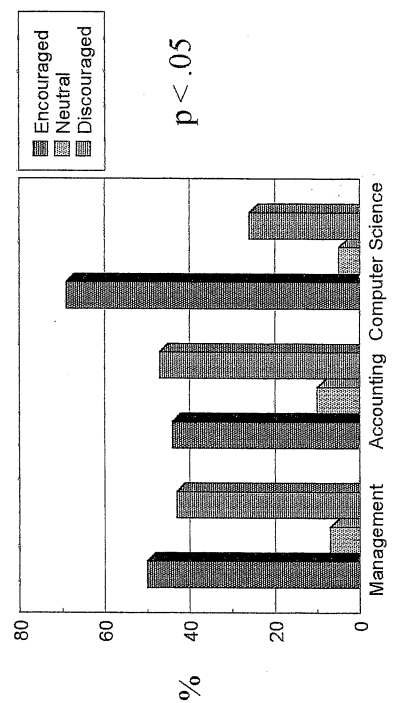


Figure 4

4. Purchased software from outside the company is not allowed on any PC.

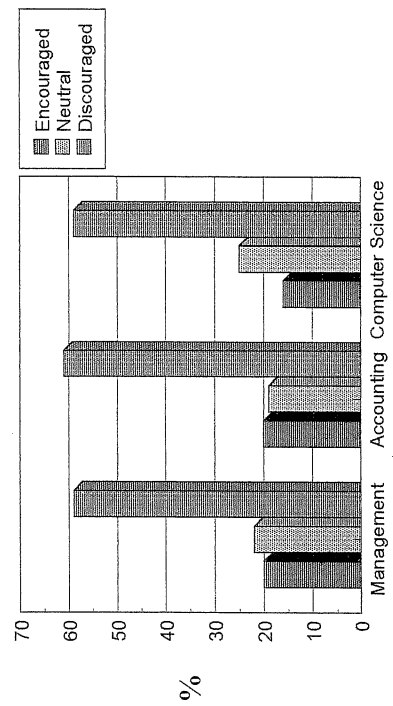


Figure 6

6. Smoking, eating, and drinking are not permitted while working on any PC.

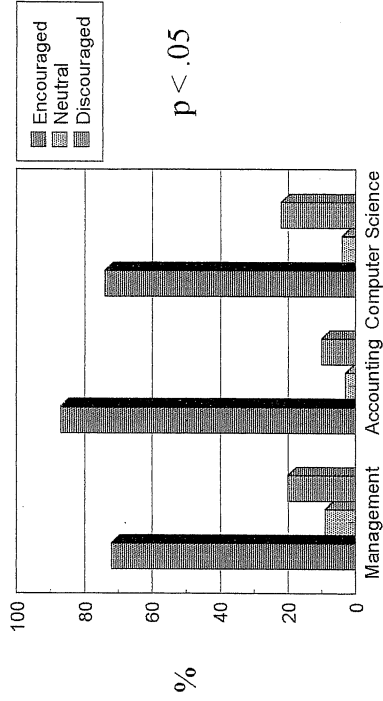


Figure 8

8. There is always a supervisor or system support personnel around to monitor and help when PC problems arise.

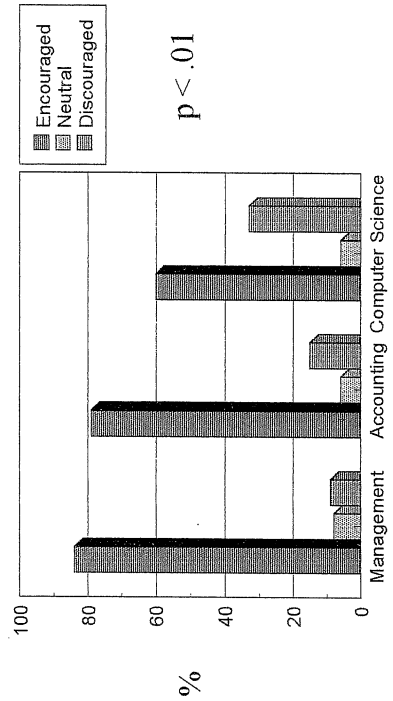


Figure 5

5. Much of the company software is menu driven with help facilities online.

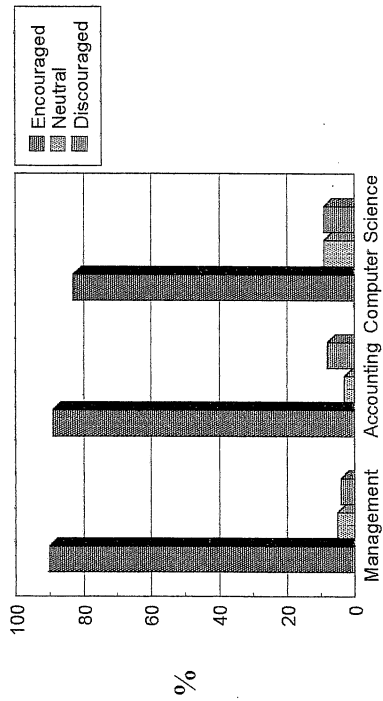


Figure 7

7. No one is permitted to use the company's PC's after normal business hours.

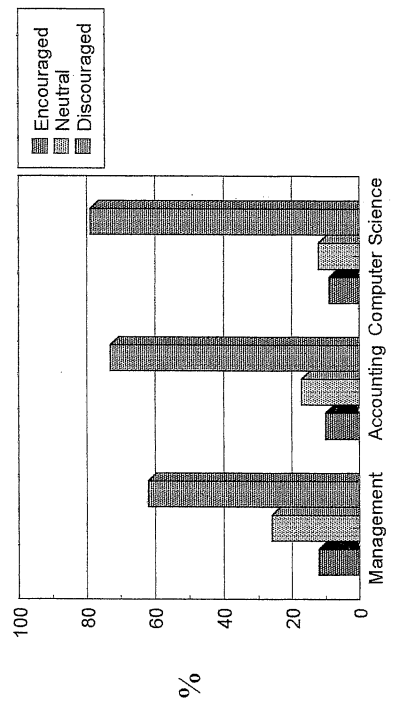


Figure 10

10. No data or program disks may be copied or removed from company premises.

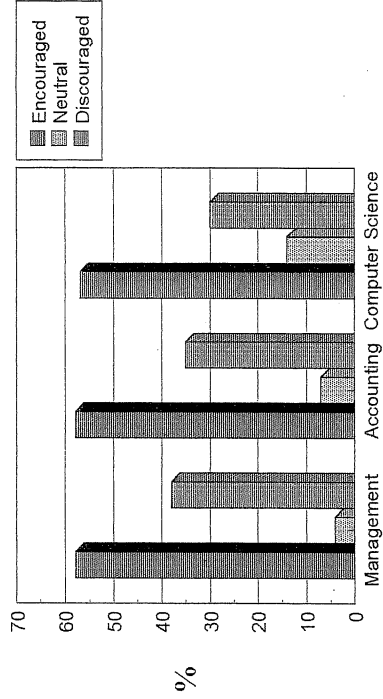


Figure 9

9. All floppy disks must be examined on a regular basis for viruses.

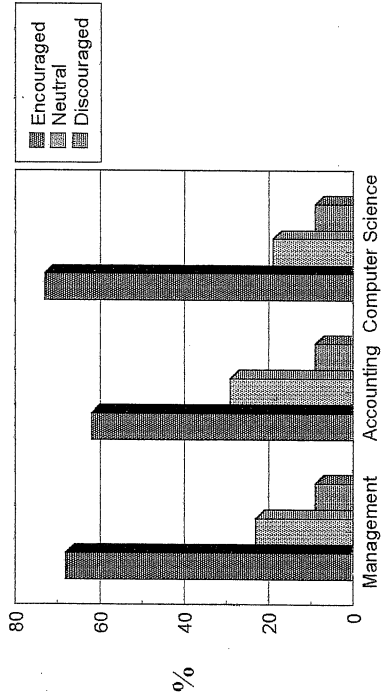


Figure 12

12. Program and data disks not being used are stored in a locked cabinet and controlled by a software manager.

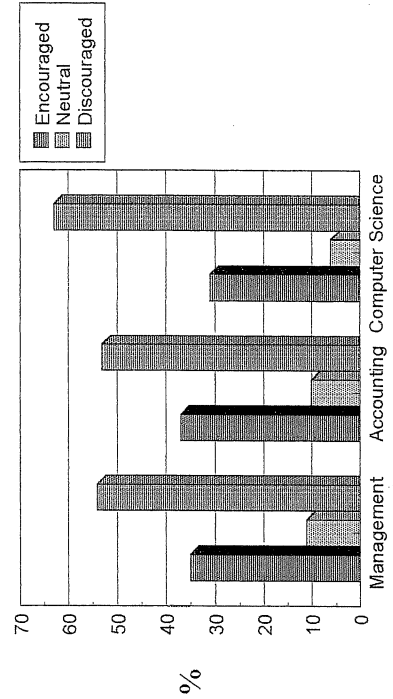


Figure 11

11. No personal use of any PC is allowed.

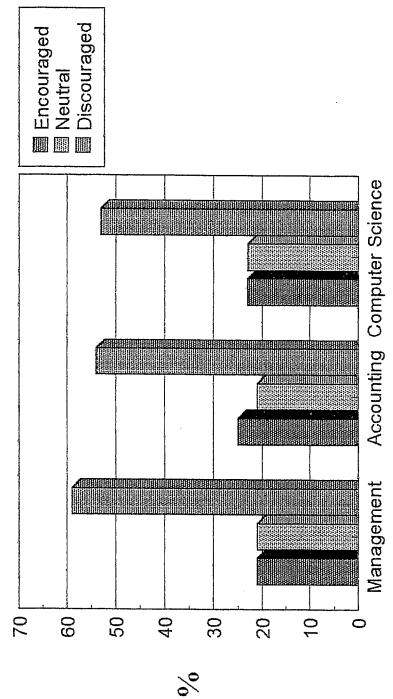


Figure 14

14. Uploading or downloading data between a mainframe and PC requires a supervisor's approval.

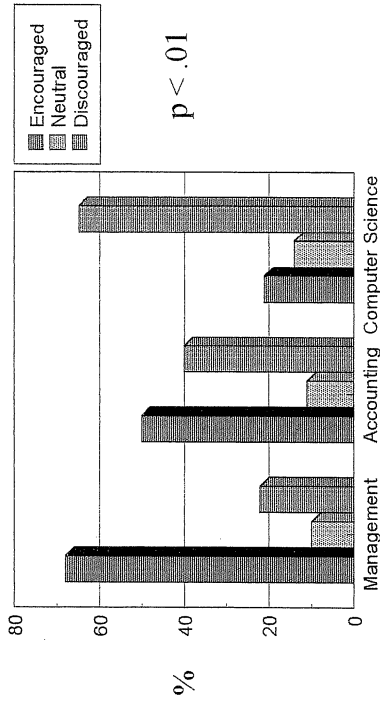


Figure 13

13. Any user developed model is not allowed to be used by other employees until fully tested and documented.

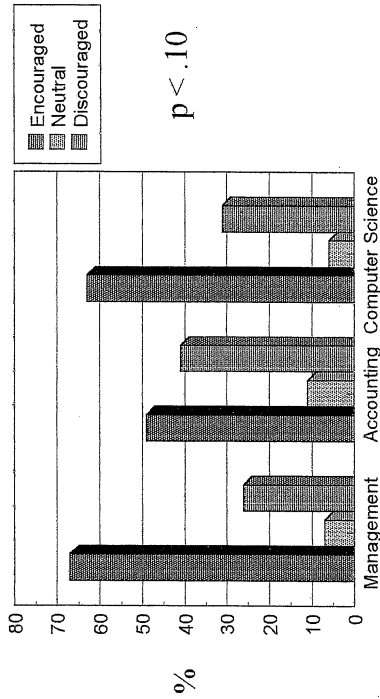


Figure 16

16. A software manager needs to be appointed to oversee all company software purchases, registrations, and licensing agreements.

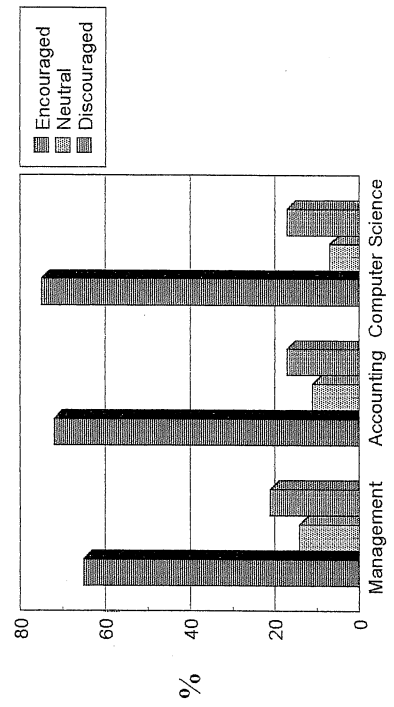


Figure 15

15. Every user must undergo a training session before being allowed on company PC's.

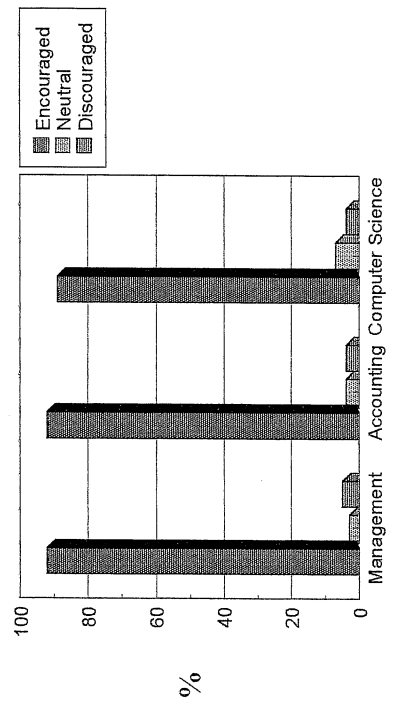


Figure 17

17. All company employees need to be familiar with a software code of ethics.

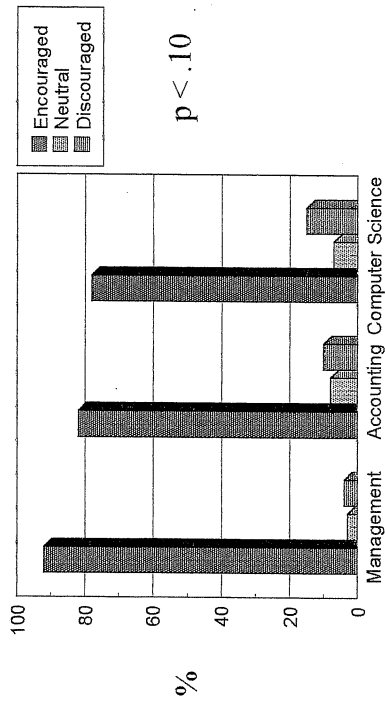


Figure 18

18. All company employees need to be familiar with software licensing agreements.

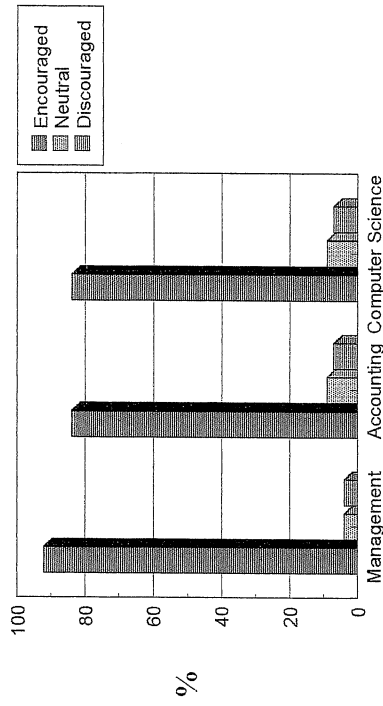


Figure 19

19. The company should audit all PC's on a periodic and surprise basis for illegal and unlicensed software.

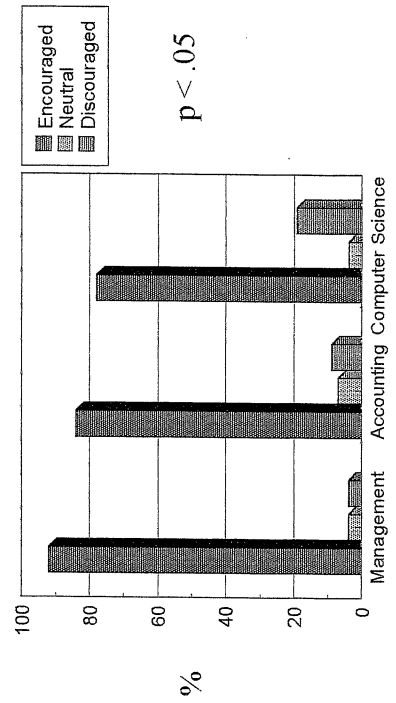


Figure 20

20. Access to a company's program and data files should be on a need-to-use basis only.

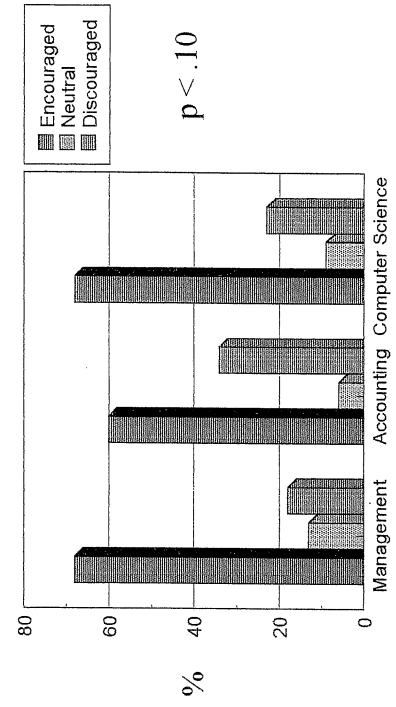


Figure 22
22. Downloading shareware or freeware from the internet requires supervisor approval and must be scanned with virus detection software.

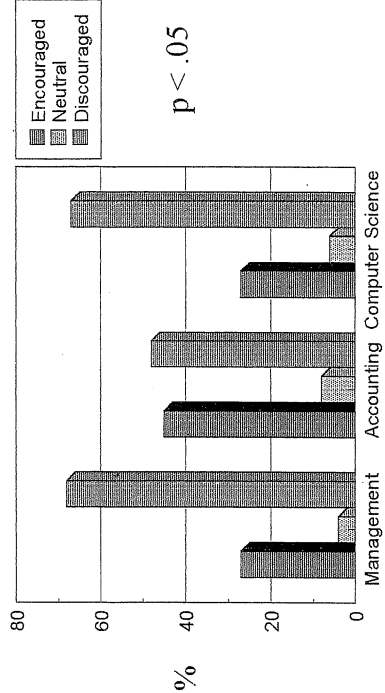


Figure 21
21. Random internet surfing is not allowed during company time.

