Accounting and Business Review
Vol. 2, No. 1, (Jan. 1995) 147-171

MANAGING INFORMATION TECHNOLOGY AMONG AUDIT KNOWLEDGE WORKERS: A CRITICAL INCIDENT ANALYSIS

Cheryl TAY
ANG Soon

School of Accountancy and Business
Nanyang Technological University

Accounting firms have invested in information technology (IT) with the belief that IT will empower auditors and produce favourable outcomes. Yet past research has shown that IT can bring about contradictory performances. The purpose of this study is to investigate the circumstances that account for differing performances in the audit environment. The study uses the critical incident technique to appropriate the work contexts in which audit knowledge workers interact with IT. Critical incidents sensitised us to relevant factors that promote or inhibit the relationship between IT and user performance. The study surfaced individual, technological, and organisational issues that management must address to improve users' ability to convert IT use into productive performance.

Information technology (IT) in organisations is growing at a phenomenal rate. A recent study reported that organisations spent about US $10,000 in IT capital on each white-collar or knowledge worker[1] (Brynjolfsson, 1993). Similarly, IT investments in accounting firms have multiplied with the dramatic increase in the use of technology in the knowledge work of auditing (Blocher, 1988).

Perhaps the greatest use of IT investments is in the area of end-user computing. In common parlance, end-user computing refers to "financial modelling, file retrieval and analysis, and the use of outside databases, all with the user in direct interactive control of the computer session" (Benjamin, 1982: 14). Driven by the low costs of hardware and availability of packaged software, end-user computing has diffused rapidly in the 1980s (McLean et al., 1993; Davis, 1988; Nadel, 1987; Weber, 1988). By late 1980s, organisations provided users with "self-service" computing environments in the form of personal workstations and standardised packaged software (Cangemi and Watson, 1989).

---

[1] A knowledge worker is a person whose work involves the use of individual and external knowledge to produce outputs characterised by information content, such as analyses, decisions, reports, etc. (Davis et al., 1991).

In fact, many firms spent between 60% to 80% of their IT budget on end-user computing activities (Amoroso and Cheney, 1991). In auditing, computer-based decision aids such as decision support systems and knowledge-based expert systems were developed for a variety of applications (Messier and Hansen, 1987; Connell, 1987; O'Leary and Watkins, 1989; Boritz and Wensley, 1992; Lehman et al., 1991). With the infrastructure for end-user computing in place, organisations anticipated benefits from IT to flow directly from knowledge workers who have become primary end-users.

Indeed, there is no dearth of literature extolling the virtues of IT use on knowledge work. A review of the accounting literature indicates a consistent belief that IT in auditing leads to improved value, efficiency, cost savings and audit effectiveness in terms of improved risk analysis, better report content and presentation, and improved audit focus in areas of high risk exposures and enhanced quality of client services (Coderre, 1993; Croft, 1992; Wolfe et al., 1989; Nadel, 1987; Tembkin, 1986; Luzi, 1981). Many also believed IT has significant indirect benefits of retaining current and attracting future clientele (Nadel, 1987).

Despite optimistic expectations about IT in knowledge work areas, evidence suggests that returns from the use of IT are not always positive. In fact, investigations on the impact of IT revealed inconsistent results at various levels of analyses, for instance, at the economy level of analysis (e.g. Roach, 1991; Osterman, 1986; Thackenkary, 1991), and at industrial level for manufacturing industries (Weill, 1990; Loveman, 1994) and service industries (Harris and Katz, 1989; Roach, 1991). Research on IT use and performance outcomes also revealed mixed and contradictory results. For instance, Farrar (1988) found user productivity to improve with IT use, while Pentland (1989) reported that IT did not improve productivity. Fripp (1985) found IT use to improve decision quality, but Aldag and Power (1986) found no such relationship. Fripp (1985) suggested that IT use could save time, yet Sharda et al. (1988) found contradictory results when they evaluated decision time and IT use.

One explanation for the inconsistent results is that these studies had adopted research methods and techniques that overly atomised the impacts of IT. By isolating the effects of IT from the people who utilised IT, researchers ignored the contextual elements embedded in real-world work environments (see Markus and Robey, 1988; Turner, 1984; Orlikowski and Robey, 1991). Managers and IT designers also tended to focus more readily on technical aspects than the social or structural dimensions of change (Mayer, 1982). Such technological deterministic or technological imperative approaches have been argued as being too simplistic as theoretical lens because they ignored the context in which IT was used, and consequently failed to examine complex social interactions between IT and organisations (Markus and Robey, 1988; Nelson, 1990). Particularly in an end-user computing environment, successful use of IT depends heavily on interactions of the individual users, technology, and the work environment (Harrison and Rainer, 1992).

We undertook this study to investigate specifically the contexts in which IT either promoted or inhibited user performance. To appropriate IT-work contextual elements, a contextualised technique -- the critical incident technique, was used and applied to external auditors from international accounting firms in Singapore.

In the following section, we present a background of the critical incident technique and its application to the study. In section 3, we present the analysis of the incidents gathered from respondents. Interpretations and implications of the study in terms of contributions to IT research and managerial practice ensue.

THE CRITICAL INCIDENT TECHNIQUE

The critical incident (CI) technique is a set of procedures for collecting contextual elements of observed episodes concerning behaviour in defined situations. Historically, the CI technique is a well known tool in psychology (Flanagan, 1949; Ericksen, 1952; Weislogel, 1952). The technique evolved from studies in the Aviation Psychology Programme of the US Army Air Forces in World War II. Since then, this qualitative methodology has been applied widely to assist in establishing standards, determining requirements, and evaluating results in areas as diverse as employee performance, workers proficiency, training, selection and classification, job design, operating procedures, equipment design, motivation, attitudes towards leadership, counselling, and psychotherapy (see Flanagan, 1954).

To date, procedures for data collection, analysis and synthesis in the CI technique have been refined into a "flexible set of principles" which when "modified and adapted to meet the specific situation at hand" can have many types of applications not limited to those mentioned above (Hedberg, 1988). The CI technique is extremely sensitive to the contexts of the respondents because respondents are asked to describe vividly the events and circumstances they experience in their current work situations. Procedures developed in the CI technique have been found to be particularly useful "for making systematic analyses of causes of good and poor performance" (Flanagan, 1947). Such procedures also have the potential for ground theory building as advocated by Glaser and Strauss (1967).

By definition, an incident means any observable human activity that is sufficiently complete in itself to permit inferences and predictions to be made about the person performing the act. To be critical, an incident must occur in a situation where the purpose or intent of the act seems fairly clear to the respondent or informant and where its consequences are sufficiently definite to leave little doubt concerning its effects (Flanagan, 1954).

The incident in this study is the use of IT in auditing, where IT refers to computers and related software. The CI technique was chosen for this study as it allows for specific observations of IT use by knowledgeable respondents. In this study, knowledgeable respondents were auditors in a real life task domain. As end-users, auditors were asked to observe and record clearly positive (experiences of outstanding work) and clearly negative (experiences of below par work) incidents on an audit assignment associated with the use of IT. Because prior literature on IT impacts indicates that sign (positive or negative) of the experience is a highly salient dimension (for example, see Attewell and Rule, 1984), positive and negative impact experiences were logical choices of critical incidents for this study.

Research Method

We adopted a survey method to implement the CI technique. Questionnaires were sent in 1991 to 534 auditors in four participating international accounting firms in Singapore. The sample consisted of all auditors in positions of staff assistants, seniors and managers in three of the four firms. For the fourth accounting firm, only seniors were included in the study as they were identified as the only set of respondents in the firm who had had any significant use of computers in audit engagements. Partners were not included in the survey as they were not primary users of IT at the time of the study. Table 1 shows a breakdown of the auditors by staff positions for which the questionnaires were sent.

TABLE 1
Responses to the Survey and Number of Positive and Negative CIs

Staff Position	No. of Individuals to whom Surveys were sent	No. of Individuals who Responded	Total No. of Reported Positive Incidents	Total No. of Negative Incidents
Managers	46	9	9	4
Seniors	116	54	51	15
Assistants	322	52	51	19
Total	534	115	111	38

A cover letter accompanied the mailed questionnaire addressed to each individual auditor. The letter explained the purpose of the study and assured respondents that responses were kept confidential. Respondents sealed their responses and returned them by mail.

The survey requested respondents to recall vividly a) incidents where outstanding work was performed with the use of computer and related software (positive incidents); and b) incidents where work was performed below par with the use of computer and related software (negative incidents). A copy of the survey form is included in Appendix A and B.

Respondents were then asked to answer specific questions for each positive and negative incident experienced in respect of the following:

1. Type of software used: respondents were asked to indicate the type(s) of computer software used during the critical incident situation and the frequency of such software use. This was to provide information about the technological component of critical situations.

2. Level of formal IT Training: respondents were requested to specify the presence or absence of IT training before usage in the incident and the duration of such training if any. This was to identify the firms' efforts in preparing auditors for using IT made available for audit engagements in the firms.

3. Nature of reinforcements for IT use: respondents were asked to indicate the rewards or punishments received for the performance reported in the critical incident(s). This was to gauge the level of firms' efforts in motivating auditors on the use of IT.

4. Nature of IT impacts: the respondents were asked to express their perceived effects of IT use. This was to elicit IT outcomes from users' perspectives in relation to specific software usage and context of use.

5. Types of attributions of IT impacts: respondents were asked to offer reasons for the IT impacts perceived in the critical incident(s). This was to obtain users' mental models of perceived causes of good and poor performance with IT usage.

Critical incidents must be studied in the light of relevant established principles of human behaviour and of the known facts regarding the background factors and conditions operating in the specific situation (Flanagan, 1954). Thus, each respondent was asked the above five categories as contextual information for studying the impacts of IT on audit knowledge work. In addition, the survey also collected respondents' demographic data that included current staff position, position tenure, organisation tenure and self-reported hours of IT use during the peak and slack seasons for the past year.

Critical incidents, by their very nature, provide self-report data. To mitigate biases arising from self-reporting, we triangulated data collection on critical incidents by conducting intensive face-to-face interviews with senior management in each of the four audit firms. Senior partners, senior managers, and seniors with substantive experience with IT in audit were interviewed at two points in time. The first series of interviews was conducted prior to the critical incident survey. Pre-survey interviews focused on obtaining relevant institutional background information about how computers and software were being used in the audit process, the functions IT played in audit, organisational results of IT use, and management's adoption and implementation strategies for IT. The second series of interviews was conducted after we have collected and analysed data from the critical incidents. Post-survey interviews were used to further our understanding and interpretation of the responses to critical incidents. Table 2 shows the time spent with senior management in the interviews.

TABLE 2
Interviews with Senior Management Pre and Post Critical Incident Survey

Staff Position	No. interviewed for Pre-CI Interview	Time taken for Pre-CI Interview	No interviewed for Post-CI Interview	Time taken for Post-CI Interview
Partners	1	1.5hrs	1	1.5hrs
Senior Manager	4	5.5hrs	4	5 hrs
Experienced Senior	1	1 hr	1	1 hr

DATA ANALYSIS AND INTERPRETATION

Sample

Table 2 shows a breakdown of the responses received from different staff positions in the accounting firms. Based on the distribution of staff positions in the original population sampled, proportionately more seniors responded (54/116 = 46.6%) compared to managers (9/46 = 19.6%) or to assistants (52/322 = 16.1%). The disproportionate number of seniors was attributable to the fact that seniors were expected to be "heavy" users of IT in the audit process. This was confirmed by the interviews with senior management of the participating firms.[2] Of the 115 auditors who responded, 34 responded to both positive and negative incidents, 77 responded to only positive incidents, while 4 responded to only negative incidents. In all, we received a total of 149 critical incidents (see Table 3).

[2] The disproportionate number of seniors should not invalidate the results of the study since the primary purpose of the study is to surface contextual factors that promote or inhibit IT use from knowledgeable end-users. In this study, seniors constitute that category of audit knowledge workers who actually use IT in their audit work, and are therefore the knowledgeable end-users.

TABLE 3
Responses to Incident Types by Staff Positions

Staff Position	Respondents who returned both positive and negative incidents	Respondents who returned only positive incidents	Respondents who returned only negative incidents
Managers	4	5	-
Seniors	12	39	3
Assistants	18	33	1
Total	34	77	4

Critical Incidents

Of the 534 surveys sent, 111 returned responses related to positive incidents, generating a 20.8% response rate, while 38% related to negative incidents, generating a 7.1% response rate.[3] A likely explanation for the relatively low response rates could be that auditors did not perceive a significant enough impact with IT usage to warrant classifying the experience as a critical incident. Nevertheless, in absolute terms, the number of positive and negative incidents should suffice for generating further research questions for in-depth study of IT impacts in the knowledge work domain.

Significantly more positive incidents were received compared to the number of negative incidents (chi-square = 52.8; $p < 0.01$). One plausible explanation is that auditors had more favourable than unfavourable experiences with IT. Another plausible explanation is that high "face-loss costs" may have deterred auditors from describing any problems they had with IT use. Especially in a society such as Singapore where virtues of IT are extolled (e.g. see Slaughter and Ang, 1994; Soh et al., 1993), it becomes even more socially undesirable for a worker in knowledge work environments to reveal negative incidents in the use of IT, and admit incompetency (or no competency) in IT skills!

The sections below provide the results of the analyses and interpretations of senior management based on the five categories of information collected from the critical incidents.

[3] According to Flanagan (1954), the number of incidents necessary for data analysis ranges from 50 to 100 incidents. In this study, we received 111 responses for positive incidents but obtained only 38 responses for negative incidents. Given the exploratory nature of the study, we feel that the numbers offer adequate insights and inputs for preliminary investigations and suggestions for management of end-user computing in the audit work environment. These results would also suffice to generate further research questions for subsequent in-depth study of IT impacts on knowledge work.

Type of Software Used. Overall, respondents reported that they used more generic software than specialised audit software. Generic software accounted for two-thirds of reported software in both the negative and positive incidents (see Table 4). Spreadsheets and wordprocessors comprise the common types of generic software used. Generic software were used primarily to facilitate structured, procedural work such as preparing workpaper schedules, and generating correspondences and memoranda.

TABLE 4
Types of Software Usage by Incident Types*

	Positive Incidents	Negative Incident
Generic Software	117	29
Specialised Software	53	20
Total	170	49

* Each incident may indicate more than one type of software usage.

Respondents reported using less of specialised audit software, accounting for only about one-third of reported software in both negative and positive incidents. Specialised audit software typically refers to customised software developed in-house by international accounting firms. In addition to the generic software capabilities of database manipulation, wordprocessing, and spreadsheets, specialised audit software also has embedded capabilities of expert systems or decision support systems specifically designed for the audit process. Specialised audit software models audit tasks and often augment or complement an auditor's judgmental and decisional skills. Examples of audit tasks modeled in specialised audit software are risk assessments, sample size assessments, and sampling decisions.

Post-CI interviews with senior management revealed that firms were only beginning to diffuse and implement specialised audit software. In fact, two of the participating firms were pilot testing specialised audit software at the time of study for mandatory implementation in the future. Thus, we would expect that, as specialised audit software becomes mandatory in future audit tasks, incidents of specialised audit software reports should increase.

Overall, the CI analysis revealed that auditor skills in IT were developed primarily to handle repetitive and routine audit tasks. Even in cases where specialised audit software was used, auditors tended to use IT to support tasks that were structured and procedural in nature. Common IT-supported structured tasks included audit procedures such as flowcharting, circularisation, and work scheduling. Relatively few respondents mentioned the use of IT for unstructured tasks of the audit process requiring decision making and judgement. Tasks that were relatively unstructured and requiring elements of audit judgement included the use of IT for risk assessment and sample size decisions.

We believe the relatively low incidence of the sophisticated use of IT in unstructured audit tasks could be attributed to two factors. One is the lack of user competence in integrating technology to less structured work of planning, decision making, and judgement. The other may be insufficient managerial support for nurturing user competence or even their use in judgement and decision making. Based on our interviews with senior management, we found those who possessed relatively limited knowledge were more conservative about the effectiveness of IT on audit work. They tended to be wary of "intelligent software" and were hesitant about relying on judgements made by an inanimate object, where the logic used by the object or system remains opaque.

In terms of types of software used associated with the types of incidents reported, we found that the proportion of generic to specialised audit software used in negative incidents was 1.45 while the proportion of generic to specialised audit software used in positive incidents was 2.21. However, a chi-square test of proportion did not reject the null hypothesis that there was no relationship between type of software and sign of incidents (chi-square = 1.59; $p > 0.05$), suggesting that type of software used was not associated with negative or positive experiences.

Level of Formal and Relevant Training in IT. Responses showed that the auditors did not receive any prior formal training for software used to perform audit work in 44% of total reported incidents (see Table 5A). This relatively low level of formal training for software use is surprising because auditing firms have always been known for their generous investments in continuous education for their most valued assets -- auditors. Training auditors on the use of computers and software to support audit work was no exception, as confirmed by the pre-CI interviews with each of the participating firms. According to senior management in the post-CI interviews, this large percentage of lack of formal training could be attributable to two major problems: timing and turnover. When audit engagement calls for the application of computer skills, auditors who were previously trained in the computer course either have forgotten how to use the software package and computer or have already left the firm. The result was that exigencies of the work situation often required assigning auditors who may not have undergone formal IT training to jobs requiring IT use as was the experience of the respondents in this study. One consequence of the mismatch of IT experience and task demands was that it has given rise to frustration to both the auditor assigned to the job and the audit firm.

Pre-CI interviews with senior management also revealed that they were more concerned with formal training for specialised audit software than for generic software. The rationale is that auditors were less likely to be exposed to specialised audit software than commercially available generic software in their prior jobs or graduate education,[4] and thus require training more for specialised audit software. Our CI study discovered that auditors underwent more specialised audit software training. The statistics showed that auditors had undergone formal training for 63% of the reported specialised audit software used on the job compared with 52% for generic audit software (see Table 5A).

In cases where auditors had undergone formalised IT training, the duration of the training sessions varied between less than a day to more than a week. The mode duration was training session that lasted no more than three days. Generally, the perception of respondents was that training, especially for specialised audit software, was inadequate for learning how to use the software effectively when performing audit tasks. The perception of inadequate training remains consistent even in cases where some audit firms offered longer training hours, e.g., more than a week, for more comprehensive specialised audit software.

TABLE 5A
Presence of Formal Training by Software Types

	Generic Software	Specialised Software
With Training	76	46
Without Training	70	27
Total	146	73

TABLE 5B
Presence of formal Training by Incident Types

	Positive Incidents	Negative Incidents
With Training	98	24
Without Training	72	25
Total	170	49

In terms of the extent of training associated with the types of incidents reported, we found that users who reported positive incidents underwent formal software training 58% of the time compared with 49% for users who reported negative incidents (see Table 5B). A chi-square analysis did not reject the null

[4] This fact is supported by a further investigation of data where several respondents alluded to university training and exposure as their fundamental hands-on experience with generic software packages.

hypothesis that there was no relationship between software training and sign of incidents (chi-square = 1.16, $p > 0.05$) suggesting that the software training was not associated with type of incidents reported.

Nature of Reinforcements for IT Use. Overall, 50% of the respondents in both the positive and negative incidents received no explicit feedback or reinforcements for their work performed with IT (see Table 6). Of the subjects who recounted positive incidents, 24% reported recognition by senior management in the form of good evaluations. Positive reinforcements were also derived from intrinsic motivation in job satisfaction and skill enhancement. In contrast, of the subjects who recounted negative incidents, 54% reported receiving poor performance evaluations as a result of the use of IT. In extreme cases, punishments went beyond mediocre performance evaluations; subjects received strong verbal reprimands for negative incidents, and were "punished" by working significant overtime to correct problems engendered from the use of IT.

TABLE 6
Nature of Reinforcements for IT Use by Incident Types

	Total	Positive Incidents	Negative Incidents
No Incentive	66 (50%)	56 (53%)	10 (38%)
Extrinsic: *poor or good evaluation, recognition or scolding*	39 (30%)	25 (24%)	14 (54%)
Intrinsic: *personal satisfaction or punishment*	26 (20%)	24 (23%)	2 (8%)
Total	131 (100%)	105 (100%)	26 (100%)

The disproportionate negative organisational feedback received for poor performance compared to positive feedback for outstanding work performed could result in demotivating auditors in their development of IT skills, experimentation with and usage of IT in their audits. In fact, user competence may well stagnate if auditors prefer to "play safe" by relying on existing manual tools and procedures rather than to experiment with software which supports planning, judgement and decision making. And, as borne out by interviews with relevant EDP audit specialists, user competence can only be enhanced via the use of planning or judgement software which offer decision support and modelling capabilities that are associated with skill enhancements such as improving and building analytical skills. Nevertheless, the presence of "punishment" may not necessarily be bad if taken in a constructive and positive light by both the evaluator and evaluatee to determine areas of improvement and action. In fact, evaluations, and especially "adverse" evaluations, may lead to future improvement of the auditors' IT competence and improved performance. What is more disconcerting was that a majority of the respondents did not receive any feedback whether for outstanding or below par performance. A direct consequence is that auditors have little information or incentive to improve on their IT skills.

Nature of IT Impacts. Subjects were asked to assess the impacts of IT use on their audit work. Impacts for negative incidents were efficiency-related. Time overruns (68%) and poor quality presentations (26%) dominated negative impacts. Other negative impacts included hindering analytical work or losing focus on the primary task of auditing (6%) (see Table 7).

TABLE 7
Nature of IT Impacts in Negative Incidents

Inefficiencies: time overruns	23 (68%)
Poor quality work: presentations, inaccuracies, etc	9 (26%)
Others: hinders analytical work, loss of focus, etc	2 (6%)
Total	34 (100%)

On the other hand, impacts for positive incidents were more varied (see Table 8). The three most commonly cited positive impacts were increased efficiency (30%); better quality presentations (26%); and improved skills, such as analytical, technical, decision and computing (19%). The remaining impacts included increased accuracy (17%), improving responsiveness to clients and client business (5%); being less dependent on others and improving confidence (3%).

TABLE 8
Nature of IT Impacts in Positive Incidents

Efficiency: time savings	68 (30%)
Quality presentations and audit outputs	60 (26%)
Improved skills: analytical, technical, decisional, computing, etc	43 (19%)
Improved accuracy: reduce errors	39 (17%)
Improved logic, responsiveness to client, overall picture of client business	12 (5%)
Others: improved confidence and independence	6 (3%)
Total	228 (100%)

The most frequently reported efficiency impact was time savings. Surprisingly, while large time savings were reported in positive incidents, a significant number (about 40%) also reported not saving any time despite experiencing outstanding performance with IT use. In contrast, respondents of negative incidents reported having lost time in every incident. Reported time wastage was considerable, with one third reporting time wastage of over 20 hours, and one over 150 hours. The fact that substantial time wastage could result from application of IT on audit jobs require firms to review their IT management strategies and staff feedback on its use.

Types of Attributions of IT Impacts. Finally, subjects were asked to offer reasons for the positive and negative IT impacts perceived in the critical incidents. Attributions for the impacts were classified into individual, technological, and organisational factors as shown in Table 9. Individual factors referred to the level and degree of personal knowledge, skill, expertise, and familiarity with IT; technological factors pertained to software capabilities in meeting client expectations, needs and audit requirements, user-friendliness and hardware capabilities; while organisational factors included user training and technical support.

TABLE 9
Number of Attributions by Factor by Incident Types

	Positive Incidents	Negative Incidents
Organisational Factors	3	6
Technological Factors	25	18
Individual Factors	18	27

In terms of an absolute number of reasons or attributions, negative incidents generated a proportionately greater number of attributions per incident than positive incidents. The average number of attributions for negative incidents was 1.3 (51/38) compared to only about .41 (46/111) for positive incidents. These numbers therefore indicated that respondents felt less need to account for positive incidents than negative incidents.

Interestingly, respondents attributed successes more to technological and organisational factors than to individual factors (28/18 = 1.6), and failures more to individual than technological and organisational factors (27/24 = 1.1). This pattern of attributional behaviour runs contrary to attribution theory (Kelley 1973) which suggests that individuals would attribute positive and negative incidents differentially. According to the theory, individuals tend to attribute positive incidents to internal causes such as individual ability or effort and to attribute failure or negative incidents to external causes such as technological or organisational factors. In this study, we found for example, that respondents attributed negative experiences to personal factors such as unfamiliarity with software (an internal cause) rather than to organisational factors such as lack of training (an external cause). It appears that respondents felt they were personally responsible for familiarising themselves with software programmes used in audit. This may be idiosyncratic of the audit work environment where independent on-the-job learning is strongly encouraged and culturally embedded in the workplace. It may also be reflective of the personal accountability pressures individual auditors face and accept in the audit environment (Lord, 1992).

Of the individual factors attributed, users' level of familiarity with the computer and related software in relation of job task was perceived as the major reason for differential IT impact on performance This is not surprising as performance is directly related to an auditors' knowledge and skills to accomplish the job.

Of the technological factors, characteristics of the software such as the level of user-friendliness, ease of use and applicability to the task at hand as well as hardware capabilities were identified as having significant impact on audit performance. Technological factors have the potential to create positive impacts depending on hardware capabilities and software applications. However, based on the critical incidents, respondents felt that focusing on technological factors alone is insufficient. Rather, real benefits are culled from the ability of the user (individual factors) to convert such technology into productive use. For example, the user is responsible to pick the appropriate software that best meets the audit and client requirement for which he has the competence.

Of the three clusters of factors, organisational factors were least attributed to by respondents. One possibility is that organisational factors, in the form of training, technical support, and organisational climate, were perceived to affect the completion of tasks only indirectly as compared to individual or technological factors. For instance, the presence of training programmes and technical support serves to improve user knowledge of capabilities (individual factors), which in turn produce desired impacts. Thus, technological and organisational factors operate as important enabling factors, creating an environment where individuals learn and improve their skills in applying IT skills to audit knowledge work.

DISCUSSION AND MANAGEMENT RECOMMENDATIONS

Evidence in this study suggests that users of software in the audit environment viewed performance impacts primarily in terms of time and cost efficiency and quality presentation. The contextual analysis of their observations showed that individual factors, specifically user competence, played the pivotal role, followed by technological factors and finally organisational factors in bringing forth performance results.

Firms must manage these three clusters of factors to minimise adverse end-user reaction, promote user competence, and ensure a favourable and positive technical and organisational environment to induce positive performance outcomes. Interpretations and implications in this section are discussed with the objective of offering useful, proactive suggestions for managing IT use among end-user computing personnel.

Management of Individual Factors

Review Recruitment and Selection Criteria. Issues such as computer aptitude, IT knowledge, skills, and competence are individual factors affecting the successful use of IT in audit knowledge work. As one senior manager observed, an individual auditor's personal interest, aptitude and inclinations toward IT can help him or her create a competence and confidence that far exceeds another who may be similarly endowed with intellectual and cognitive abilities but without that personal IT aptitude or interest. One major implication for the audit firms adopting IT intensively in audit engagements is to review existing recruitment and selection criteria and ensure that auditors with sufficient IT competencies are recruited.

Manage Interplay of Technological and Organisational Factors. In addition, auditors with IT abilities must be motivated to use IT. As we know from Vroom (1964) and others, job performance is not only a function of a person's ability but a multiplicative function of both a person's ability and his or her motivation. Thus, besides careful recruitment and selection, firms can do more by managing motivation through the interplay of the technological and organisational factors to provide the necessary environment to encourage building user competence, confidence, knowledge and skills in the use of IT on the job.

Management of Technological Factors

Invest in Appropriate and Adequate Technology. Because IT has the potential to contribute to positive impacts, the firm has the responsibility to ensure appropriate and adequate acquisition of hardware and software technologies. Unavailability of computers was one of the reasons given for negative impacts. Inadequate number of computers can affect trialability (Rogers 1983), limiting opportunities to "play" and interact in the IT environment which is necessary to build confidence and task skills as well as speed and accuracy. Cost considerations and high rate of obsolescence in hardware technology were reasons offered by the firms for modest acquisitions of hardware. Nevertheless, with proper planning and innovative scheduling of available hardware, firms can overcome this problem. For instance, some firms encourage ownership of computers by making available firm loans. One accounting firm even implemented a policy where auditors could purchase older hardware equipment relatively inexpensively when the firm upgraded their computers to newer, portable models. Loans of office machines can also be made available for those who do not own one. Software programmes should also be made available for personal practice whether in or outside office.

Thorough Review of IT to Match Work Objectives. Interface problems and incompatibility of existing office hardware as well as software limitations were other commonly cited reasons for negative results. Software limitations refer to inability to meet audit task objectives. These problems are indicative of lack of management foresight and inadequate understanding of the IT environment. To minimise these adverse impacts on end-users, senior management need to take considerable steps to plan carefully and evaluate needs to ensure such future problems do not occur. For instance, adequate evaluations of software programmes whether generic or specialised must be carried and re-customised to meet the local context where necessary before adoption. Trial implementations for selected audit jobs where computer competent auditors are assigned could help highlight areas of concern. The next concern of the management is then the diffusion of capable technology, i.e., how to encourage auditors to use and reap benefits from their use. Careful management of organisational factors can accomplish this.

Management of Organisational Factors

Review Frequency of Training. Formal training affects an individual's computer-related ability (Nelson and Cheney, 1987) and is a basic requirement for imparting new IT skills and knowledge in the audit firms. Analysis and discussions above on the level of formal and relevant IT training indicate that more needs to be done to mitigate the adverse effects of assigning auditors who may not have undergone IT training on audits requiring the use of IT.

As with other audit training and development courses, computer courses are typically scheduled only once a year during the slack period in the external audit work environment. Firms can conduct ongoing, ad hoc refresher short courses to meet specific end-user requirements. These could be carried out informally as and when the need arises within the audit groups or across all audit groups. Nevertheless, individual auditors have the responsibility to take the initiative to create opportunities to learn new technologies and prevent IT skills erosion.

Make Audit Software Available for Practice in Formal Educational Environment. The analysis on IT training also indicate that training for specialised audit software was inadequate despite more firms' efforts to provide formal training on the use of such software. To promote greater competencies in idiosyncratic software, audit firms could proactively promote the use of such software in formal educational environments. For example, in other business contexts such as banking, software houses developing and supporting specialised packages promote trialability as a means of diffusing the use of a specific software. Specifically, software houses actively promote and demonstrate the use of the specialised software, offer considerable financial incentives and staff support to universities to ensure that future knowledge workers gain the experience, skills and competence in specialised packages. Similarly, accounting firms could actively promote trialability by permitting universities and other formal audit educational institutions access to specialised audit packages to train and educate potential audit employees. Exposure to software packages helps potential auditors overcome psychological barriers in dealing and working with computers before they become attitudinal barriers in actual work environment. Exposure during formal education also allows them greater latitude to learn and gain deeper appreciation of the technological capabilities without having to justify time costs. Finally, exposure at a younger age is also an advantage in terms of responsiveness to the challenges of new technologies and in gaining basic competence and expertise in IT usage (Harrison and Rainer, 1992).

Allow for Self-Paced IT Learning. Results of the critical incident analysis also suggest that the "quantity" of formal training, in itself, may not be sufficient in building user competence. In other words, increasing the period or length of formal training may not be a solution. Rather, firms must understand the pedagogic principles of end-user IT learning and use in the "high-tech workplace" (see Schuck, 1985; Gattiker, 1992). In fact, appropriate training strategy that matches individual's attitudes toward computer-mediated work is necessary to increase the transfer of learning to the job (Gattiker and Hlavka, 1992). Programmes that cater for hands-on and simulation practice as well as availability of self-tutoring programme for self-learning at the user's own pace could be valuable in meeting different individual learning needs. Informal training in the form of on-the-job and off-the job training is another viable option. Informal training constitutes a major portion of nurturing user competence by having them learn the software, both generic and specialised on the job, by the experimental "trial and error" basis.

Implement and Improve Technical Support/Help Teams. In addition to issues relating to training, respondents also alluded to inadequate technical support. Post CI interviews with senior management revealed that accounting firms have indeed implemented structures to improve technical support. For instance a number of firms have instituted self-help teams within audit groups, and special support team. Nevertheless, respondents were either ignorant of these groups, or found such "local experts" or self-help personnel with skills which did not meet their task requirements. One important implication for audit firm is that more needs be done to improve the visibility of such support groups, to pick the right and qualified personnel to comprise this team. Availability of these support teams should preferably be "on-line", i.e., available when required. On-line help is especially crucial for auditors who require assistance during the initial implementation of IT use (such as the adoption of new audit software) until a sufficient critical mass of competence in their usage has been attained.

Promote Conducive IT Environment. Finally, a conducive work environment can promote user competence. For instance, Schuck (1985) suggests that firms should create an environment of inquiry, in which managers manage the learning process rather than giving orders, to assist workers to go beyond routine performance and contribute to business results. One suggestion is that management consider using a more conscious strategy of organisational reinforcement to promote IT skill development, user competence, positive IT attitude and users' IT sophistication beyond the basic skills of applying IT to structured, procedural tasks. Incentives (which need not be monetary but in the form of recognition and affirmation) can motivate performance and skill development (Lawler, 1991) and may be necessary to maintain a positive attitude towards IT use. It has been found that a negative attitude towards computer use can contribute to negative impact on user performance (Harrison and Rainer, 1992). A regular, proper appraisal and evaluation programme to continually assess, monitor and provide feedback to the auditors on their competence levels, and training requirements coupled with appropriate incentives can help. Incentives to ensure auditors maintain and upgrade their computer knowledge and skill with provision of refresher and new software programmes much like their continuing educational programmes will help promote positive individual factors.

CONCLUSION

The study demonstrates how via the critical incident technique, a rich descriptive analysis of the use of IT by end-users in their own work domain can offer a valuable opportunity in understanding the associations and causes of user behaviour and performance. Specifically, through the use of contrasting incidents, both positive and negative, we can surface and assess problems faced by users in their attempts to integrate IT to their work environment. Based on the critical incident analysis, we found that the successful use of IT depends primarily on the skills and abilities of the users. Furthermore, although organisational and technological factors may be insufficient by themselves to bring about desired impacts, their presence are nevertheless, important contributing or intervening factors in generating performance. These factors are also within the control of the management; these factors include technological issues such as selection of compatible software and organisational issues such as promoting the acquisition of competent future users and developing a learning atmosphere. Firms should thus do more to manage proactively the interplay of these factors which is critical in ensuring a workforce which can work and integrate IT productively into their knowledge work domains.

APPENDIX A
Clearly Positive Incident

Everyone has experiences of doing exceptionally good work. Think of an audit assignment you worked on in the past 12 months when it was clear to you that your work with the use of microcomputers was outstanding. Keep in mind that experience and answer the following questions. Please be specific and be sure to answer every question.

Type of Software Used

1. Which computer software programme(s) did you use in this assignment?

2. How frequently did you use the above-mentioned software in your audit assignments in the past 12 months? Circle one of the numbered responses below:

1	2	3	4	5
frequently		sometimes		seldom

Level of Formal IT Training

3. Have you had training with the above-mentioned software? When and for what duration.

Nature of IT Impacts

4. How and in what ways did the use of software in this assignment lead you to believe you performed exceptionally well? Please describe in technical details.

5. When you were doing that exceptionally good job, which audit skills do you believe were enhanced with the use of the software.

6. Did you feel that besides accomplishing the audit tasks, the use of software directly or indirectly assisted you in spotting new organisational or internal controls which you could recommend to the client? Please elaborate.

7. How did this experience where you believed you had performed exceptionally well affect the way you do your job?

8. How would you rate the effect this experience will have on your future use of the microcomputer and future performance at work? Circle one of the numbered responses below:

1	2	3	4	5
no effect		some effect		very large effect

Types of Attributions of IT Impacts

9. What do you think were the reasons you performed well in this assignment with the use of the software?

Nature of Reinforcements for IT Use

10. How were you rewarded for accomplishing what you believe was an exceptionally good job with the use of the software?

APPENDIX B
Clearly Negative Incident

Everyone has experiences of doing exceptionally good work as well as experiences of performing below par. Think of an audit assignment you have worked on in the past 12 months when it was clear to you that your work with the use of microcomputers was not as good as it could have been. Keep in mind that experience and answer the following questions. Please be specific and be sure to answer every question.

Type of Software Used

1. Which computer software programme(s) did you use in this assignment?

2. How frequently did you use the above-mentioned software in your audit assignments in the past 12 months? Circle one of the numbered responses below:

1	2	3	4	5
frequently		sometimes		seldom

Level of Formal IT Training

3. Have you had training with the above-mentioned software? When and for what duration.

Nature of IT Impacts

4. How and in what ways did the use of software in this assignment lead you to believe you performed below par? Please describe in technical details.

5. When you were doing that work that was below par, which audit skills do you believe were hindered by the use of the software.

6. Did you feel that besides accomplishing the audit tasks, the use of software directly or indirectly hindered you in spotting new organisational or internal controls which you could recommend to the client? Please elaborate.

7. How did this experience where you believe you had performed below par affect the way you do your job?

8. How would you rate the effect this experience will have on your future use of the microcomputer and future performance at work? Circle one of the numbered responses below:

1	2	3	4	5
no effect		some effect		very large effect

Types of Attributions of IT Impacts

9. What do you think were the reasons you performed below par in this assignment with the use of the software?

Nature of Reinforcements for IT Use

10. How were you reprimanded for accomplishing what you believe was work performed below par because of the software?

REFERENCES

Aldag, R. J., and Power, D. J. 1986. An empirical assessment of computer-Assisted decision analysis. ***Decision Sciences,*** 17(4): 572-588.

Amoroso, D. L., and Cheney, P. H. 1991. Testing a causal model of end-user application effectiveness. ***Journal of Management Information Systems,*** 8(1): 63-91.

Attewell, P., and Rule, J. 1984. Computing and organizations: What we know and what we don't know. ***Communications of the ACM,*** 27(12): 1184-1192.

Benjamin, R. 1982. Information technology in the 1990s: A long-range planning scenario. ***MIS Quarterly,*** 6(2): 11-31.

Blocher, E. 1988. Using microcomputers in auditing. ***Journal of Accountancy,*** 128-134.

Boritz, J. E., and Wensley, A. 1992. Evaluating expert systems with complex outputs: The case of audit planning. ***Auditing: A Journal of Practice & Theory,*** 11(2): 14-29.

Brynjolfsson, E. 1993. The productivity paradox of information technology. ***Communications of the ACM,*** 36(12): 67-77.

Cangemi, M. P., and Watson, R. D. 1989. How auditors can use computers. ***Practical Accountant,*** 22(3): 24-31.

Connell, N. 1987. Expert systems in accountancy: A review of some recent applications. ***Accounting and Business Research,*** 17: 221-233.

Coderre, D. G. 1993. Automating the audit function. ***Internal Auditor,*** 50(5): 18-20.

Croft, M. 1992. Let the computer take the strain. ***Accountancy,*** 110(1187): 60-61.

Davis, K. W. 1988. A new world of PC-based generalized audit software. ***CPA Journal,*** 58(12): 97-103.

Davis, G. B., Collins, R. W., Eierman, M., and Nance, W. D. 1991. ***Conceptual model for research on knowledge work.*** Working Paper Series, Management Information Systems Research Center, University of Minnesota, Minnesota.

Ericksen, S. C. 1952. Development of a light plane proficiency check to predict military flying success. ***USAF, Human Resource Research Center Tech. Rep.,*** 52-6.

Farrar, R. L. Jr. 1988. Cost-benefit analysis of an automated system. ***Business Credit,*** 90(5): 28-30.

Flanagan, J. C. 1947. The aviation psychology program in the army air forces. ***AAF Aviation Psychological Program Research Rep.,*** 1.

Flanagan, J. C. 1949. A new approach to evaluating personnel. ***Personnel,*** 26: 35-42.

Flanagan, J. C. 1954. The critical incident technique. ***Psychological Bulletin,*** 51(4): 327-358.

Fripp, J. 1985. How effective are models? ***OMEGA: The International Journal of Management Science,*** 13(2): 19-28.

Gattiker, U. E. 1992. Computer skills acquisitions: A review and future directions for research. ***Journal of Management,*** 18(3): 547-574.

Gattiker, U. E., and Hlavka, A. 1992. Computer attitudes and learning performance: Issues for management education and training. ***Journal of Organizational Behaviour,*** 13: 89-101.

Glaser, B., and Strauss, A. 1967. ***The discovery of grounded theory.*** Chicago: Aldine.

Harris, S. E., and Katz, J. L. 1989. Predicting organizational performance using information technology managerial control ratios. ***Proceedings of the Twenty-Second Hawaiian International Conference on System Science,*** Honolulu, Hawaii.

Harrison, A. W., and Rainer, R. K. Jr. 1992. The influence of individual differences on skill in end-user computing. ***Journal of Management Information Systems,*** 9(1): 93-111.

Hedberg, P. R. 1988. ***Individual Perceptions of Performance Feedback in a Work Setting.*** PhD Dissertation, Department of Psychology, University of Minnesota.

Kelley, H. H. 1973. The processes of causal attribution. ***American Psychologist,*** 28: 107-128.

Lawler, E. E., III 1991. The design of effective reward systems. In R. M. Steers and L. W. Porter (Eds.), ***Motivation and Work Behaviour,*** 507-531. (5th ed.). Princeton, NJ: McGraw Hill.

Lehman, M. W., Malley, J. C., and Cassidy, J. 1991. Expert systems for audit planning: Strategies for local accounting firms. ***Woman CPA,*** 53(3): 14-17.

Lord, A. T. 1992. Pressure: A methodical consideration for behavioral research in auditing. ***Auditing: A Journal of Theory & Practice,*** 11(2): 89-108.

Loveman, G. W. 1994. An assessment of the productivity impact on information technologies. ***Info Technological and the Corporation of the 1990s,*** 84 -110. New York: Oxford University Press.

Luzi, A. D. 1981. ***Computers in the audit process: Current issues.*** Working paper, Pennsylvania State University.

Markus, L., and Robey, D. 1988. Information technology and organizational change: Causal structure in theory and research. ***Management Science,*** 34(5): 583-598.

Mayer, R. R. 1982. ***Social science and institutional change.*** Transaction Books, New Brunswick, NJ.

Messier, W. F. Jr., and Hansen, J. V. 1987. Expert systems in auditing: The state of the art. ***Auditing: A Journal of Practice and Theory,*** 7: 94-105.

McLean, E. R., Kappelman, L. A., and Thompson, J. P. 1993. Converging end-user and corporate computing. ***Communications of the ACM,*** 36(12): 79-91.

Nadel, R. B. 1987. Computer auditing: Has its time come? ***The CPA Journal,*** 57(3): 24-29.

Nelson, D. L. 1990. Individual adjustment to information-driven technologies: A critical review. ***MIS Quarterly,*** 14(1): 87-98.

Nelson, R. R., and Cheney, P. H. 1987. Training end users: An exploratory study. ***MIS Quarterly,*** 11(4): 547-559.

O'Leary, D. E., and Watkins, P. R. 1989. Review of expert systems in auditing. ***Expert Systems Review,*** 2: 3-22.

Orlikowski, W. J., and Robey, D. 1991. Information technology and the structuring of organizations. ***Information Systems Research,*** 2(2): 143-169.

Osterman, P. 1986. The impact of computers on the employment of clerks and managers. ***Industrial and Labor Review,*** 39: 175-186.

Pentland, B. T. 1989. Use and productivity in personal commuting: An empirical test. ***Proceedings of the Tenth International Conference on Information Systems,*** 211-222. Boston, Massachusetts.

Roach, S. S. 1991. Services under siege -- the restructuring imperative. ***Harvard Business Review,*** 82-92.

Rogers, E. 1983. ***The Diffusion of Innovation.*** (3rd ed.). New York: Free Press.

Schuck, G. 1985. Intelligent technology, intelligent workers: A new pedagogy for the high-tech work place. ***Periodicals Division, American Management Association,*** 66-79.

Sharda, R., Barr, S. H., and McDonnell, J. C. 1988. Decision support system effectiveness: A review and empirical test. ***Management Science,*** 34(2): 139-159.

Slaughter, S., and Ang, S. 1994. Employment structures of information systems professionals: A comparative study of the United States and Singapore. ***Proceedings of the SIGCPR 1994 Conference,*** 24-26. Washington, D. C.

Soh, C., Neo, B. S., and Markus, M. L. 1993. State-wide strategic planning for IT: A critical appraisal of the Singapore IT2000 project. ***Journal of Strategic Information Systems,*** 2(4): 351-371.

Tembkin, R. H. 1986. Automating auditing: Auditing will never be the same. ***Corporate Accounting,*** 4(4): 56-59.

Thackenkary, C. S. 1991. Information technology expenditure and U.S. productivity: On the fundamentals of an information economy. ***EDI Europe,*** 1(2): 153-168.

Turner, J. 1984. Computer mediated work: The interplay between technology and structured jobs. ***Communications of the ACM,*** 27(12): 1210-1217.

Vroom, V. H. 1964. ***Work and Motivation.*** New York: Wiley.

Weber, R. 1988. ***EDP Auditing.*** (2nd ed.). NY: McGraw-Hill.

Weill, P. 1990. ***Do Computers Pay Off?*** ICIT Press, Washington, D. C.

Weislogel, R. L. 1952. Critical requirements for life insurance agency heads. ***University of Pittsburgh Bulletin,*** 48: 300-305.

Wolfe, C., Bain, C., and McPheters, W. 1989. Microcomputer productivity in the internal audit function: A case study. ***The Ohio CPA Journal,*** 48(1): 12-16.