Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 1998 Proceedings

Americas Conference on Information Systems (AMCIS)

December 1998

Impact of Advances in IS on Audit Quality and Audit Technology

Ramesh Kini
The Hong Kong University of Science and Technology

Impact of Advances in IS on Audit Quality and Audit Technology

Ramesh G. Kini
Department of Information and Systems Management
The Hong Kong University of Science and Technology

Introduction

While quality has always been important for accountants in general, and the Big Six (Five) in particular, it is even more so now. With the acute changes that have taken, and are taking, place, audit quality should have become even more pivotal in the firms' quest for "growth, glamour and profitability," and not as tangential or even irrelevant as it has ostensibly become according to some critics of the profession, e.g., Stevens (1991). Perhaps, the profession, that historically epitomized quality in its "guardian of the public interest" role, has not really become as complacent about quality as it is being made out to be. It is impossible, we feel, for any technology that relies solely on inspecting a client's books *ex-post* to be *perfect* and *100% reliable* (in terms of being able to: discriminate *perfectly* between a Warren Buffett and a Barry Minkow-type[1] fraudster; and detect *each and every* Minkow *before it is too late*) and yet affordable. As diligent and healthily skeptical as auditors are, they can at best deliver a high quality—but <u>not</u> perfect —service, just like the assurance provided by any test or system for screening library patrons, airline baggage, etc.

Elliott (1994) saw the recent advances in IT as enabling an expanded assurance function that aims at reducing the decision makers' information risk through reliable, timely, relevant and complete (financial/nonfinancial) information and transcends the normal attestation of, say, published financial reports. Highly-publicized audit-failures and "the draining cost of litigation still unanchored to responsibility for fault," as Elliott (1994) put it, do affect the reputation of the profession and the firms' audit practices—this will probably catalyze change of another sort: using IT to move away from the traditional *ex post* inspection and towards continuous, offline audit quality assurance. Specifically, we see intelligent agents (see, e.g., Knapik and Johnson, 1998) being used as tireless watchdogs that the client can-not influence, and which will filter transactions on a real time, ongoing, exhaustive, boundary-less, non-intrusive, non-obtrusive basis, and envisage users of information (e.g., banks, analysts, institutional/individual investors) paying for the assurance provided, instead of the clients.

The Model—Lessons from Manufacturing

After studying, evaluating and reviewing the client's internal control system and testing for compliance with it, auditors usually conduct two other substantive tests or audit procedures: ("top-down") analytical procedures and ("bottom-up") tests of details. We can assume, w.l.o.g., that internal auditors can find and correct any errors in the books, that all material misstatements are attributable to fraud, and that the auditors—based on the red flags[2] that come to light during the engagement in such a case—can probe further for more evidence to support their decision, e.g., to qualify. It is not surprising, however, that some red flags are willfully ignored, given that: i) the increasing commoditization of traditional attest services has led to greater downward pressure on audit fees and on cost- and time-budgets, accordingly; ii) relying on screening and substantive tests that are less than perfectly sensitive or specific results in both false negative and false positive errors; and that iii) a false positive error's costs are *surely* borne in the form of time and effort "wasted" during the engagement on investigating further those red flags that turn out to be "red herrings," while the false negative error's costs would *probably* have to be borne afterwards if the firm is found liable for any going concern failures.

Let A denote a positive test or an alarm going off as in any library, indicating that something is amiss about the accounts being audited, or that a patron was trying to leave with library material that ostensibly had not been checked out; and $\overline{A}$ a negative test or a no-alarm state, implying that the accounts are seemingly problem-free or that the patron is "clean." Let D $(\overline{D})$ indicate that, in reality, the client is a Minkow (a Warren Buffett), or that the patron is dishonest (honest), respectively. The test or alarm system meets "spec." if: i) it catches a Minkow or a dishonest patron in the act (probability $P(A \mid D)$ is the test's *<u>sensitivity</u>*); and ii) a Buffett or an honest patron is not unduly hassled $P(\overline{A} \mid \overline{D})$ is the test's *<u>specificity</u>*). It fails if: iii) with probability $P(\overline{A} \mid D) = 1 - P(A \mid D)$. a Minkow is misdiagnosed as "clean"; or iv) a Buffett is subjected to further, unwarranted scrutiny with probability $P(A \mid \overline{D}) = 1 - P(\overline{A} \mid \overline{D})$. We will focus mainly on the posterior probabilities, *viz.*, that of a: iii´) *<u>false negative</u>* error, $z^{-} = P(D \mid \overline{A})$, and iv´) *<u>false positive</u>* error, $z^{+} = P(\overline{D} \mid A)$.

[1] Fraudsters like Cortess Randell and Barry Minkow (who were jailed in the NSM and ZZZZ Best cases, respectively; see Malkiel, 1996, and Stevens, 1991) may not have gotten away with as much, as brazenly, and for as long, as they did, had it not been for the credibility bestowed on them by the auditors standing on the sidelines, with "wool pulled over their eyes."

[2] While "red flag" has traditionally had specific connotations (in the sensxe of SAS Nos. 6, 16, 17, etc.; see, e.g., Elliott and Willingham, 1980), here the term refers more loosely to a test's positive outcome or any event that triggers off alarm bells.

Let, say, one in a thousand clients (library patrons) be dishonest with *mala fide* intentions, i.e., *P(D)* = 0.001 and $P(\overline{D})$ = 0.999, and the test or alarm system's sensitivity and specificity values be 98% and 99%, respectively. The false negative and false positive probabilities can easily be obtained as: $z^{-} = P(D\,|\,\overline{A}) = 0.00002$ and $z^{+} = P(\overline{D}\,|\,A) = 0.91067$, respectively. While the z^{-} value is fairly low, the client or patron "caught" seems nearly always to be of the wrong sort. Sensitivity (specificity) gains help reduce the false positive- and false negative-probabilities (since $\partial z^{+}/\partial P(A'|'D) < 0$, $\partial z^{+}/\partial P(\overline{A}\,|\,\overline{D})<0$, $\partial z^{-}/\partial P(A\,|\,D) < 0$, and $\partial z^{-}/\partial P(\overline{A}\,|\,D) < 0$ hold), but the impact is not the same in each case, e.g., $z^{+}(z^{-})$ is marginally lower by a mere 0.16% (0.99%, respectively) for a perfectly sensitive (specific) system or test. On the other hand, sensitivity (specificity) gains affect $z^{+}(z^{-})$ very significantly, i.e., as sensitivity (specificity) → 1, $z^{+}(z^{-})$, respectively) → 0.

The basic tradeoff can be spelt out as follows. Unless the system works perfectly, consistently, and under all circumstances, some Minkows will succeed, on the one hand, in "cooking the books," just as some bombs will probably make it past the baggage scanner. On the other hand, the problem's "needle in a haystack" flavor implies that the fewer the dishonest library patrons, Minkows, or terrorists, the more likely will the system's false positive errors lead to honest, decent patrons, clients, or travelers being harassed needlessly. As often seen in practice, such errors significantly increase the load on the inspection and rework stage, but are ignored unlike false negative errors, because their ramifications for others are less serious.

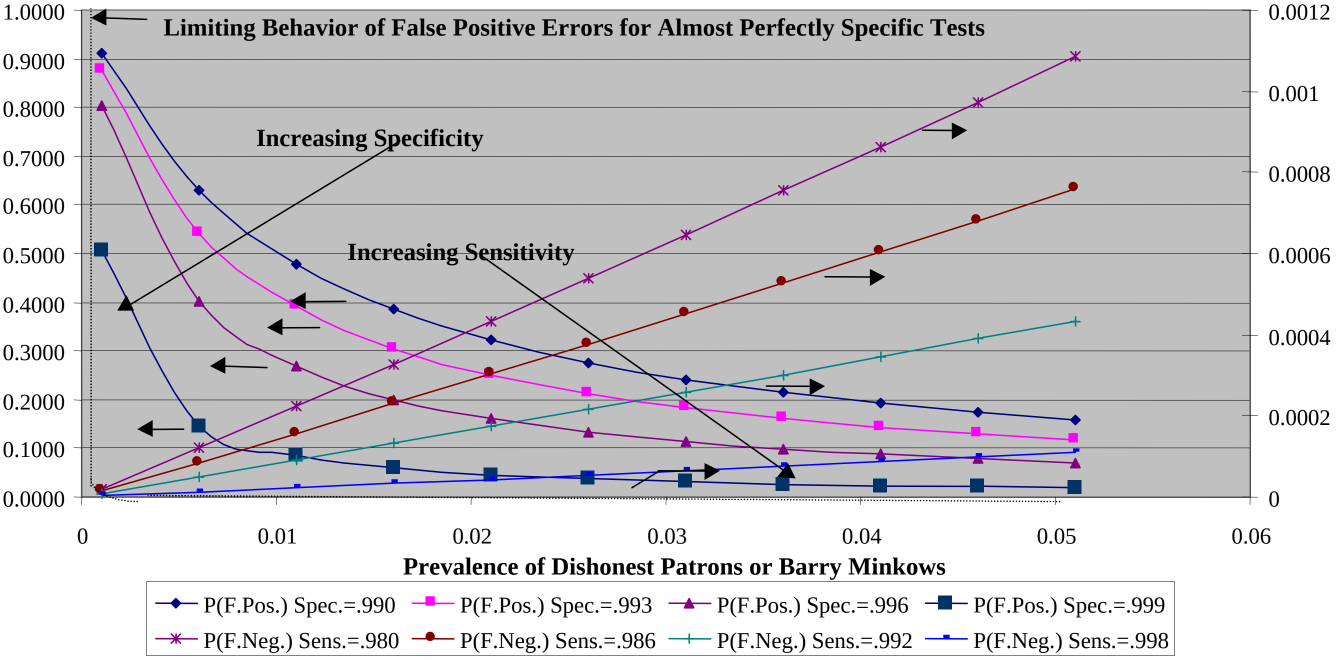

Figure 1. The Effect of the Base Rate on the False Positive and False Negative Error Probabilities

Lastly, *P(D)* the base rate or prevalence of Minkows in the population, also affects audit quality. As Figure 1 shows, $\partial z^{-}/\partial P(D) > 0$ and $\partial z^{-}/\partial P(D) < 0$ hold—more importantly, $z^{+} \rightarrow 0$, as $P(D) \rightarrow 0$, for any less-than-perfectly-specific test or alarm system. This effect leads to significant increases in inspection, scrap and rework costs for manufacturing firms, who—on realizing that they can-not inspect their way past 3- quality levels all the way down to zero-defects, or even 6-levels—have switched from reactive inspection, to designing quality proactively into the product and process, as suggested by, e.g., Dr. Deming. Similarly, relying on more—or more intensive—manual auditing (*via* longer engagements, a bigger staff, etc.), or more refined sampling techniques, would increase people-related and other overhead costs pro-portionately, as depicted in Figure 2, making this approach too costly, both for the auditor and the client. But, is there any alternative?

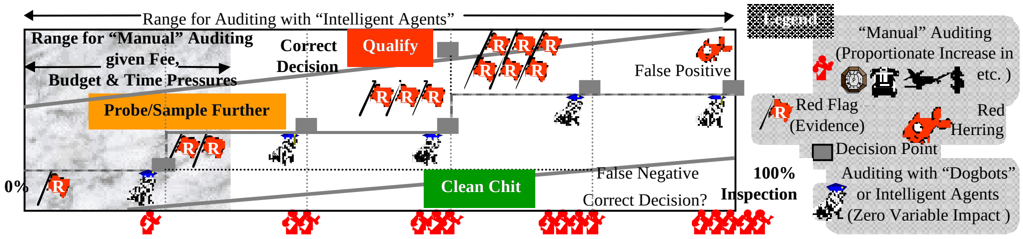
Range for Auditing with "Intelligent Agents"
Range for "Manual" Auditing given Fee, Budget & Time Pressures
Correct Decision
Qualify
False Positive
Probe/Sample Further
0%
Clean Chit
False Negative
Correct Decision?
100% Inspection
Legend
"Manual" Auditing (Proportionate Increase in etc.)
Red Flag (Evidence)
Red Herring
Decision Point
Auditing with "Dogbots" or Intelligent Agents (Zero Variable Impact)
R

Figure 2. End-of-Year "Manual" Auditing vs. Continuous Auditing Using "Dogbots," with Sequential Sampling

Using Intelligent Watch-Dogs (Dogbots)

To ensure that no Minkow or Randell can get away with fraud, auditors will have to be more than professionally and healthily skeptical in their approach. That is, moving from SAS No. 16 to SAS No. 54 may not be enough. If the null hypothesis is flipped over, i.e., every potential client is *a priori* thought of as a Minkow in the making, z^{-} would coincide with the base case's Type I (and not Type II) error. Further, this would also address the confirmation bias issue that psychologists (e.g., Klayman and Ha, 1987) have raised. What implications does beginning with the basic *adversarial* premise that every client is potentially a Minkow have for the auditor, the audit technology and the client? While the prospect of not being able to slide any financial "curved balls" past an utterly-skeptical auditor would keep the would-be-Minkows-if-given-half-a-chance along the straight and narrow, how would it affect most of the other clients who are honest? Would it not antagonize the Warren Buffetts and Andy Groves who typically far outnumber the Minkows and Randells among the firm's clients? The audit technology would have to be *pervasive* and yet inherently *non-invasive* and *non-obtrusive*.

Suppose the auditor could deploy intelligent agents as watch-dogs (dogbots or Westland dogbots, after J. Chris Westland, a colleague, who had suggested that I "look at AI"; cf., softbots) that reside passively within the client's system. Such dogbots could: get activated each time an entry is made into the system; check and *validate* the entry *both internally and externally*; and do so *in real time*, *non-invasively*, *non-obtrusively* and *on an ongoing basis*. External validation would come in the form of valid responses to the queries posed by the mobile agent sent by the auditor's supervisory system across the Internet to the client's supplier's or customer's system, as shown in Figure 3. Such a response could be elaborate, or of the simple yes /no form. In either case, quantities supplied/sold, the prices and terms for the transaction in question, can also be cross -checked and authenticated at the other end by the client's supplier's/customer's auditor—who would also have to be kept in the loop—thus allowing for *boundaryless* auditing. Since corresponding entries could thus be vetted at both ends (e.g., quantity shipped with that received, receivables with payables, etc.), both firms/auditors would benefit symmetrically. Ad hoc queries may have to be on a strictly billable basis. A disinterested third party, say a CHIPS-like automated information clearing house, could handle, for a small fee, the routing of queries and responses, the encryption process, billing, etc. Network externalities would require issues relating to access protocols, inter-operability, security, compliance with standards, etc., to be addressed so as to allow for universal applicability.

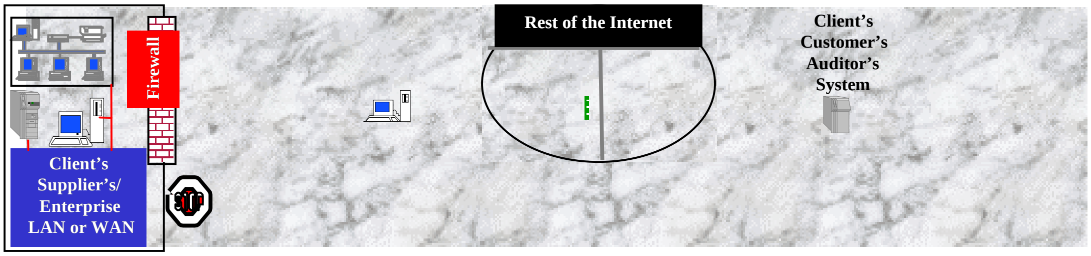
Rest of the Internet
Client's Customer's Auditor's System
Firewall
Client's Supplier's/ Enterprise LAN or WAN

Figure 3. The Use of Dogbots for Continuous, Real Time, Exhaustive, Boundry-less, Non-Obtrusive Auditing

Such a system would not be prone to gullibly accept such palpably fabricated evidence as the From-Nick-and-Lisa fax in the Barings case. Such a watch dog would also be less prone to being duped by someone within the firm (as in the Wicke's DIY chain case) unless collaborators at the supplier's/customer's end of the transaction could be induced to likewise "fudge" their figures, so as to evade detection by their auditor's dogbot—an impossible task in a truly networked world, with no sink holes or cul-de-sacs along the information superhighway, if all auditors were to act in concert. With mostly fixed costs—borne upfront and not recurring—and a negligible marginal cost of ensuring quality on an ongoing basis (given the recent/expected drops in computing costs and free/nearly-free access to the Internet), such a system could, therefore, afford to monitor the client's books *exhaustively*, i.e., on a 100% sampling basis (as in Figure 2), *continuously*, *costlessly*, and so on.

At the risk of sounding flip, this author offers "Dogged dogbots can do the dog-work involved in auditing, without getting dog-tired; so let them," as a solution to the audit quality problem. Such a system would: i) simplify the task of attestation by obviating the need for, e.g., analytical procedures; ii) make actual users (investors, creditors, etc.) pay (through linear/nonlinear, single/multi-part tariffs) for real-time, attested, financial/non-financial information—see arrows marked (2), in Figure 3—providing the client with some relief in this regard; and iii) come a lot closer to ensuring total audit quality than the extant manual system, or the more recent applications of AI (*viz*., the large and unwieldy rule based expert systems that tried to mimic the human auditor, instead of delegating time-consuming, routine and costly tasks to machines as described above). To conclude, this approach would allow for the assurance/ attest function to be expanded more comprehensively and more profitably than is currently being envisaged.

References

References are available upon request from the author (imkini@usthk.ust.hk).