1987

# An Analysis of Techniques for Risk Assessment

Paul Caster
*pcaster@fairfield.edu*, pcaster@fairfield.edu

Published Citation

Caster, Paul. "An Analysis of Techniques for Risk Assessment," The EDP Auditor Journal 3, (July 1987): 30-38.

# THE EDP AUDITOR JOURNAL
## VOLUME III, 1987

THE INFORMATION SYSTEMS CONTROL FOUNDATION

# THE EDP AUDITOR JOURNAL

An International Journal
Published quarterly by
THE EDP AUDITORS FOUNDATION, INC.

Editor: Michael P. Cangemi, CPA, CISA

Director of Publications: Laura Mockus Van Gemert

International Headquarters:
P.O. Box 88180
Carol Stream, Illinois 60188-0180, U.S.A.
312/653-0950

The EDP Auditor Journal is published by The EDP Auditors Foundation, Inc. (EDPAF), a non-profit organization created for the public by The EDP Auditors Association, Inc. (EDPAA), in 1976. Membership in the EDPAA, a voluntary organization of persons interested in electronic data process (EDP) and auditing, entitles one to receive The EDP Auditor Journal and The EDP Auditor Update and to purchase Association Publications at membership rates.

*Printed in U.S.A.*

# AN ANALYSIS OF TECHNIQUES FOR ASSESSING RISK

by
Paul Caster

## I. INTRODUCTION

Contingency planning has received a great deal of attention in the past fifteen years as organizations have grown more and more dependent upon the computer. Catania, Dick and Silverman (1980) define a contingency plan as "a description of the actions to be taken, the resources to be used and the procedures to be followed, before, during and after an unlikely event occurs that renders inoperative an organization's data processing capability" (p. 3).

Several authors discuss the need for contingency plans [see, for example, Logan (1985), Copeland and McClure (1984), Comer (1983), Weights (1982) and Cerullo (1981)]. Fish and Morrissey point out that "a comprehensive contingency plan can mitigate the effects of (disasters that) . . . cause the loss of computing power" (1984, p. 1). They cite a study that estimated that "typical losses for a manufacturing company with $215,000,000 in annual sales would be approximately $94,000 during the first business week after the disaster, $879,000 after the second week, and $2,400,000 by the end of week three" (p. 2) assuming no alternative data processing capability. Some contingency planning articles stress the point that management has been lax in developing such plans. For example, Freedman states that "some disaster recovery experts place the number of adequately prepared organizations at close to five percent" (1983, p. 106).

A number of approaches have been suggested in the literature for development of contingency plans. Three basic elements common to all such approaches are: (1) identification of risks, (2) quantification of risks and (3) assessment of the probability of occurrence of each risk identified. Identification of risks is perhaps the easiest of the three to accomplish. A number of authors provide fairly comprehensive checklists. For example, Martin (1973, pp. 12-13) provides a table of 39 "security risks" that would be common to most computer installations. Once risks have been identified, they need to be quantified in terms of frequency and amount of loss. This is often referred to in the literature as "risk assessment," and it is the focus of this paper. Specific concerns include how risks are quantified and how probabilities are determined.

The paper is organized as follows: Section II contains a review and critique of risk assessment techniques that have been suggested in the literature. In Section III, some findings in behavioral science relative to risk assessment are discussed. Section IV is a *preliminary* investigation into the possible applicability of risk assessment techniques in computer installations to the situation in auditing of assessing audit risk. Conclusions are contained in Section V.

## II. RISK ASSESSMENT TECHNIQUES

A number of risk assessment techniques have been suggested in the literature. Some are specifically aimed at contingency planning and others have been developed in an auditing context. The techniques are organized below in chronological order and are identified by authors.

### Martin (1973)

As mentioned in the introduction, Martin (1973, pp. 12-13) identifies 39 security risks. He also provides examples of the probability of occurrence of each risk, using an 8-point scale ranging from "virtually impossible" to "might happen 10 times a day." Martin cautions that the estimated probabilities are merely examples and "will differ from one installation to another" (p. 14). No guidance is provided on how to establish estimated probabilities. However, Martin states that only crude estimates are required.

Martin also suggests an 8-point scale for the estimated cost of damage, ranging from "negligible" to "on the order of $10,000,000." Since the book is now 13 years old, his scale may have to be adjusted. Martin warns that occurrence of each of the 39 security risks may not be independent of each other, so that simply multiplying probabilities would not be appropriate.

The main criticism of Martin's technique is that it is highly subjective. Although it provides the rudiments of risk assessment, it is lacking in specific guidance as to how probabilities and amounts are determined and whether determination can be made more objectively. It is clearly a heuristic approach. For example, there is no theoretical basis for the 8-point scales that are suggested.

### Fitzgerald (1978a, 1978b)

Fitzgerald advocates "the matrix approach to risk analysis (1978a, p. 4). The approach involves six steps which are combined into a matrix that displays assets (in rank order) and possible threats to each asset. According to Fitzgerald, estimating "the probability of each threat's occurrence . . . is the most difficult step" (1978a, p. 3). He suggests use of the Delphi Technique, which he describes as follows: The "best and most knowledgeable management personnel . . . (meet in) face-to-face discussions (and) pool their expertise to arrive at (estimated probabilities of occurrence for each threat)" (1978a, pp. 2-3). The Delphi Technique is also recommended to arrive at "consensus" estimates of the dollar amounts of each asset, if "lost."

As for determining (and ranking) the possible threats facing each asset, Fitzgerald recommends "brainstorming" sessions. Users, auditors and data processing personnel meet and threat scenarios are elicited "no matter how far-fetched or ridiculous they may seem" (1978b, p. 2).

Fitzgerald's approach is practical and the Delphi Technique makes it far less likely that one individual ultimately determines the estimates. In other words, consensus estimates of several experts are likely to be more accurate (and less biased).

There are three problems, however, with Fitzgerald's approach. One problem is that the estimates are highly subjective. Suppose, for example, that a competitor's computer center is destroyed by fire. Management decides to establish a contingency plan because there is now concern about the possibility of fire. If Fitzgerald's approach is followed, the probability of fire will probably be overestimated because it is so salient.

The second problem underlies the matrix approach. It assumes independence of events (recall Martin's warning). If two (or more) threats are not independent, the joint probability is not simply the product of the two individual probabilities.

The third problem is mentioned as a postscript to Fitzgerald's (1978a) article. There is reason to be concerned about making employees aware of "a virtual inventory of data processing vulnerabilities" (1978a, p. 8). It is suggested that this could actually *increase* risk.

**Mair, Wood and Davis (1978)**

The approaches covered thus far are from a management perspective. Mair, Wood and Davis (1978) take an auditing perspective. The authors recommend that auditors use a control evaluation table to assess risk. The control evaluation table provides a single cause of exposure, such as losing a check, the types of exposures that result from a given cause and the controls in force that reduce the likelihood of occurrence of a given cause. A different table is prepared for each cause.

Mair, Wood and Davis (1978, pp. 13-15) suggest the use of two 4-point rating scales in conjunction with the control evaluation tables. Each control is rated from "very reliable" to "no significant use." The magnitude of each exposure is rated from "virtually certain" to "very unlikely."

The major benefit from using a control evaluation table approach is that it highlights controls in place (or the lack thereof) that act to mitigate the likelihood of various threats. The major weakness in this approach is that it is highly subjective. The two 4-point scales recommended are very crude and subject to differing interpretations. Also, no dollar amounts are incorporated into the tables.

**Cerullo and Shelton (1980)**

Cerullo and Shelton (1980) combine Martin's (1973) approach and the control evaluation table approach[1] and extend the analysis to consider the cost and benefit of various controls. They start by identifying 59 possible threats in four categories. Threats are ranked by likelihood, using Martin's approach; and the expected loss is calculated. Next a control evaluation table is prepared and various control strategies are ranked in terms of importance to management. The cost of each control is determined in terms of its implementation cost and its yearly operating cost. Furthermore, the authors recommend that the reliability of

[1] The authors provide an example of a control evaluation table and cite Touche Ross and Company as its source. The table shown is identical in format to the Mair, Wood and Davis (1978) control evaluation table approach, though it was not cited by the authors. It is unclear as to who originated the idea of control evaluation tables, but in this paper it is assumed to be the Mair, Wood and Davis source previously cited.

each control be assessed and incorporated into the cost analysis. For example, what is the additional expected lost if a given control fails? Finally, an optimal mix of controls is chosen. The optimal mix is defined as the "point where the total expected cost of the control combinations is at a minimum or the net worth is at a maximum" (p. 63).

Although Cerullo and Shelton provide two illustrations of their technique that make the calculations appear relatively easy, they gloss over the difficult parts of the process, e.g. where do all of the figures used come from? Their "quantitative evaluation" technique appears to be fairly objective at first glance, but it is actually quite subjective and subject to the same criticisms that were made of Martin's approach. They incorporate Martin's heuristic approach for the assessment of probabilities, but fail to mention Martin's warning regarding possible non-independence of threats. Cerullo and Shelton's technique can also be criticized for employing the same crude, 4-point scales to evaluate controls that were discussed in Section II.

The main contribution of Cerullo and Shelton (1980) is the cost/benefit analysis of controls. A computer installation should not incorporate every conceivable control. An optimal mix of controls that incorporates the cost of controls as well as the benefits is clearly preferable.

**Perry (1981, 1984, 1985)**

Perry recommends "a risk analysis technique using multiples of 10 for impact and frequency" (1981, p. 56). The risk analysis matrix is very similar to Martin's (1973) approach. The main difference is that Perry suggests ranges of frequencies in multiples of 10 (e.g., once per year, ten times per year, etc.) and ranges of dollar impacts in multiples of 10, starting with the lowest impact (e.g. $1, $10, $100, etc.). Like Martin, Perry warns that "loss is often associated with a sequence or chain of conditions or events" (1981, p. 13) which makes a more straightforward analysis problematic. The matrix approach suggested, however, does not address this problem.

Perry goes further than Martin in that he discusses how to arrive at entries in the cells of his risk analysis matrix. He suggests the use of "interviews and analysis . . . (to decide upon) a range of values into which most analysts agree the determinants (of risk) should fall" (1981, pp. 83-84). Presumably, this would not preclude use of the Delphi Technique suggested by Fitzgerald (1978a).

Perry modifies his suggested approach in later writings. For example, in Perry (1984), he suggests just four levels of probability (5%, 25%, 50% and 75%) which are clearly not multiples of 10. In a major departure from expected value theory, Perry also states that if the dollar amount of risk is significant, "the auditor should test the controls over that risk area, *regardless of its occurrence probability*" (1984, p. 5, emphasis added). Although this is written from an audit perspective, it still contradicts the expected value theory underlying the risk analysis matrix in Perry (1981), which is also written from an audit perspective.

In Perry (1985), the concept of vulnerability analysis is introduced. Each application system is evaluated from the standpoint of the effect of downtime and its impact on the organization. Four levels of downtime are evaluated, 1 day, 1 week, 1 month and indefinite. Perry also suggests an evaluation of how critical each system is for each level of downtime. "The degree of criticality is rated as high, medium, or low" (1985, p. 2).

The concept of vulnerability analysis is an important contribution to contingency planning and the audit of computer installations. However, for the most part, Perry's approach is not that much different from Martin (1973). Using multiples of 10 does not seem to add much to Martin's framework. (Recall that Martin used 8-point scales.) Again, as with all techniques previously discussed Perry's is highly subjective. Using relative terms, such as "high" or "medium," results in different interpretations and therefore different evaluations by different auditors.

**Friedman (1984)**

One of the first authors to take a more objective approach to risk assessment and the development of contingency plans is Friedman (1984). Friedman uses actual data from an IBM study covering 352 disasters over an 11-year period. It is interesting to note that fire caused nearly half of all disasters during the period. Theft was the next largest category accounting for 17% of the disasters in the study.

Friedman also reports the average time period, in days, that companies in various industries were able to continue essential functions following a data center disaster. The range is 2 days for financial firms to 5.6 days for insurance companies.

The rest of Friedman's article is concerned with aspects of a contingency plan that are unrelated to the topic of interest in this paper. Although Friedman does not discuss risk assessment techniques per se, the evidence reported in his article could be used by others to determine estimated probabilities on a much more objective basis than the previous techniques used.

**Mohr and Ruckh (1985)**

Mohr and Ruckh "present a methodology that has been used in a major banking firm to assess the risks associated with computerized systems and their human-machine interfaces" (1985, p. 1). They state that the "objectivity of risk analysis procedures reduces misunderstandings and leads to more cost-effective decisions" (p. 1). Unlike all previous articles reviewed, Mohr and Ruckh are quite cognizant of the limitations in risk assessment techniques and they list four limitations for the methodology presented in the paper. The limitations apply to all of the techniques reviewed, therefore, they are reproduced in Table 1.

There are two phases involved in the Mohr and Ruckh methodology. The first phase involves a preliminary review that is designed to determine the exposures and their relative levels. The authors suggest the use of control evaluation tables based on those developed by Mair, Wood and Davis (1978). However, the ratings are eliminated from the tables and the primary purpose is to categorize exposures and possible offsetting controls.

The next step in the preliminary review is to prepare three 3-by-3 matrices,

**TABLE 1:**
**LIMITATIONS OF RISK ASSESSMENT TECHNIQUES**
**from**
**Mohr and Ruckh (1985)**

1. The risk scenarios developed are limited by the creativity and ingenuity of the team members and are not all-inclusive.
2. Data regarding the probability of a fraud is limited and may be too imprecise to be reliable.
3. No reliable method exists for distributing the combined probability of a fraud over all scenarios developed. Each scenario must therefore be given an equal probability of occurrence, which tends to overstate the identified risks.
4. Development of risk scenarios by a threat analysis team increases individual awareness of methods to circumvent existing controls and may increase the risk of a fraud occurring.

one for impact (the "magnitude of a possible loss"), one for value (the "marketability of the threatened asset") and one for likelihood. The values in the cells are "based on organization or industry experience" (pp. 4-5). The authors point out that these are only preliminary figures used to determine the relative exposure.

The next step is the preparation of an overall exposure matrix. Each system is "ranked from highest to lowest (exposure) using a forced-choice approach" (p. 5). System exposures are determined by totalling the values from all of the matrices.

The second phase of the analysis is referred to as "detailed risk analysis." Only the highest ranked systems in terms of exposure are subjected to the second phase in this approach. Significant breaks in the rankings or standard deviations are suggested to determine the cutoff point for which systems are further analyzed in phase 2. Much of the work in this phase is similar to Fitzgerald's (1978a) approach, in that threat scenarios are devised in "brainstorming" sessions. The authors suggest that risk analysis personnel "work with management to quantify the potential dollar loss and probability of occurrence" (p. 10). They properly note that this part of the task is highly subjective, but they believe that accurate objective data for probabilities is not generally available.

The next step recommended is the calculation of annual expected exposure values, which can be summed to determine the total risk for a given system. Like Perry, the authors are concerned that expected values, particularly where the dollar amounts are very large but the probabilities are very low, may be misleading. Therefore, they suggest that both the total dollar amount of the exposure as well as the expected exposure after multiplying by the probability be reported to management. The remaining steps are beyond the scope of this paper.

The methodology presented in Mohr and Ruckh is a combination of the best aspects from most of the techniques reviewed in the previous sections. It is somewhat disappointing, however, that the authors seem to suggest that more objective evidence be used in the preliminary review phase than in the detailed risk analysis phase. Other than that, however, the technique seems practical and is probably "the state of the art" in risk assessment in the area of contingency planning.

## III. BEHAVIORAL CONSIDERATIONS

Fischoff, Slovic and Lichtenstein (1978) report the results of a series of experiments on the structure of fault trees that seems particularly relevant to computer risk assessment. A fault tree is a method of diagramming how things can go wrong. Branches of the tree can be used to indicate the probability of occurrence. The nodes can be used to indicate amounts. The authors point out that fault trees have been used "in the design of technological systems from spaceships to nuclear power plants" (p. 332). They also state that "fault trees are . . . used to estimate failure rates for complex systems when historical data for the system as a whole are unavailable" (p. 332). In short, the fault tree methodology seems particularly well suited for risk assessment.

Three aspects of fault tree structure were studied by the authors: (1) how much detail is left to the "all other causes" category, (2) how much detail is presented and (3) how systems are "grouped into branches" (p. 332). They found that the subjects in their experiments were not sensitive to what was left off of a fault tree (and thereby presumably a part of the "all other causes" category). This resulted in distortions of the estimated probabilities of the various branches. When the experiment was revised so as to focus subjects' attention on the all other causes branch, the authors found "little effect," i.e., it "improved their awareness, but only partially" (p. 336). One wonders, therefore, if the threat scenario brainstorming sessions recommended by Fitzgerald and others suffers from the same sort of bias.

The second question studied, varying the level of detail presented in the branches, produced no measurable effect.

The third question was studied in an experiment called "splitting and fusing branches." The authors found that "the more pieces into which a system of failure pathways is organized, the more important that system seems" (p. 340). This bias does not appear to be relevant to the techniques described in Section 2, but should be kept in mind if a fault tree approach is used in contingency planning.

While most of the experiments used students as subjects, it is interesting to note that one experiment was replicated using experienced subjects. The same bias relating to the distortion of probabilities caused by variations in what is left out of a fault tree was found in this experiment.

## IV. ASSESSING AUDIT RISK

One of the objectives of this research was to determine if risk assessment techniques used for contingency planning in a computer environment could be applied to the assessment of audit risk. Plesser (1984) provides a brief review of SAS No. 47 on audit risk. He states that "audit risk is defined as the risk that the auditor may unknowningly fail to appropriately modify his opinion on financial statements that are materially misstated" (p. 83).

There are three components to audit risk: (1) inherent risk, (2) control risk and (3) detection risk. Plesser defines these as follows:

> Inherent risk is the susceptibility of an account balance or class of transactions to error that could be material . . . Control risk is the risk that a material error could occur which would not be prevented or detected on a timely basis by the system of internal control . . . . Detection risk is the risk that an auditor's procedures will not disclose a material error. (p. 84)

From the above definitions, it is clear that assessing audit risk is quite different from the computer environment. For example, it is unlikely that many generalized procedures can be developed for audit risk. It is difficult to imagine a checklist such as Martin's (1973) that would be of much use in this situation. In fact, Reiter states that "inherent risk varies not only from financial statement item to financial statement item, but also by financial statement assertion. Therefore, to assess inherent risk, auditors have to consider the financial statement item, inventory, say, and the specific assertion under examination attached to it—existence, for example" (1984, p. 47).

On the other hand, assessing control risk seems very adaptable to the Mair, Wood and Davis (1978) concept of control evaluation tables. As for detection risk, a fault tree might be a useful way to examine various audit procedures and to estimate how they might fail to detect material errors under a variety of circumstances.

All in all, based on a very preliminary review, it would appear that risk assessment techniques in the computer environment do not lend themselves to easy adaptation for the assessment of audit risk, except for the control evaluation tables previously mentioned. Reiter (1984) suggests a Bayesian revision strategy, which does seem well suited to the task, especially given the nature of audit evidence. Cunningham (1984) and Godier (1984) each suggest that audit risk can be assessed using mathematical formulas. The results of their analysis can then be used to budget audit time so as to reduce the overall risk. It would appear that much work remains to be done in the area of assessing audit risk.

## V. CONCLUSIONS

Over the last decade, several risk assessment techniques have been proposed as part of contingency planning in a computer environment. The early approaches are characterized by: (1) a lack of theoretical basis, (2) the use of heuristics, (3) possible systematic biases (e.g., due to salience of threats) and (4) highly subjective estimates. Starting with somewhat crude matrices of amounts of loss and estimated probabilities, control evaluation was added [Mair, Wood and Davis (1978)], cost/benefit analysis was suggested [Cerullo and Shelton (1980)], the Delphi Technique was recommended [Fitzgerald (1978a)] and the concept of vulnerability analysis was introduced [Perry (1985)]. More recently, there has been a call for more objectivity in the analysis [Friedman (1984) and Mohr and Ruckh (1985)].

To date, the fault tree methodology has not appeared in the contingency planning literature; however, it seems particularly appropriate for the task. If fault trees are employed, the behavioral findings of Fischoff, Slovic and Lichtenstein (1978) should be considered.

Finally a preliminary review of audit risk assessment was performed. It appears that the nature of audit risk is considerably different from risk in a computer environment. Also, it seems unlikely that risk assessment techniques developed for the latter can be adapted to the problem of assessing audit risk.

## REFERENCES

Catania, Salvatore C., Walter J. Dick and Martin E. Silverman. *Contingency Planning: A Discussion of Strategies.* U.S.A.: Coopers and Lybrand, 1980.

Cerullo, Michael J. "Accountants' Role in Computer Contingency Planning." *The CPA Journal* (January 1981), pp. 22-26.

——— and Fred A. Shelton. "Quantitative Evaluation: A New Way to Measure Computer Security." *CA Magazine* (October 1980), pp. 57-66.

Comer, Mike. "Contingency Planning—and the Audit." *Accountancy* (March 1983), pp. 58-61.

Copeland, Eric A. Jr. and James M. McClure. "Information System Contingency Planning—A Business Approach." *EDP Journal* (1984), Volume 1, pp. 25-31.

Cunningham, Terry. "Audit Planning by Risk Index." *Public Finance and Accountancy* (September 1983), pp. 32-33.

Fischoff, B., Paul Slovic and Sarah Lichtenstein. "Fault Trees: Sensitivity of Estimated Failure Probabilities to Problem Representation." *Journal of Experimental Psychology: Human Perception and Performance* (1978), pp. 330-344.

Fish, Toni and Douglas Morrissey. "DP Backup and Recovery Alternatives." In *Data Security Management: Auerbach Information Management Series,* Pennsauken, New Jersey: Auerbach Publishers, Inc., 1984, Number 85-01-01, pp. 1-7.

Fitzgerald, Jerry. "EDP Risk Analysis for Contingency Planning." *Edpacs* (August 1978a), pp. 1-8.

———. "Developing & Ranking Threat Scenarios." *Edpacs* (September 1978b), pp. 1-5.

Freedman, David H. "Are You Ready for a Disaster." *Infosystems* (October 1983), pp. 106-112.

Friedman, Stanley. "Contingency and Disaster Planning in EDP." *Edpacs* (January 1984), pp. 4-9.

Gardner-Brown, Magdalena. "Auditing the 'Disaster' Risk Area." *Accountancy* (March 1983), pp. 62-64.

Godier, Dwayne P. "Automated Audit Risk Analysis." *EDP Auditor* (1984), pp. 21-28.

Logan, Andrew J. "Contingency Planning." In *EDP Auditing,* Pennsauken, New Jersey: Auerbach Publishers, Inc., 1985, Number 73-05-20, pp. 1-13.

Mair, Wlliam C., Donald R. Wood and Keagle W. Davis. *Computer Control and Audit.* Sarasota, Florida: The Institute of Internal Auditors, 1978.

Martin, James. *Security, Accuracy, and Privacy in Computer Systems.* Englewood Cliffs, New Jersey: Prentice Hall, Inc., 1973.

Mohr, Joseph H. and Patrick Ruckh. "Risk Analysis of Software Systems." In *EDP Auditing,* Pennsauken, New Jersey: Auerbach Publishers, Inc., 1985, Number 73-01-14, pp. 1-12.

Perry, William E. *Computer Control and Security.* New York: John Wiley and Sons, 1981.

———. "Auditing the Data Center: An Introduction." In *EDP Auditing.* Pennsauken, New Jersey: Auerbach Publishers, Inc., 1985, Number 76-06-10, pp. 1-11.

———. "Testing Data Center Controls." In *Data Center Operations Management: Auerbach Information Series.* Pennsauken, New Jersey: Auerbach Publishers, Inc., 1984, Number 41-07-03, pp. 1-11.

Plesser, Daniel. "Audit Risk and Materiality." *The CPA Journal* (July 1984), pp. 83-85.

Reiter, Carolyn. "Risk Assessment: An Important Part of the Audit." *CA Magazine* (July 1984), pp. 47-49.

Weights, Philip J. "A Methodology for Evaluating Contingency Planning." *Edpacs* (October 1982), pp. 1-7.