XI-6

DP Insurance: A Management Tool

Mark Schindel
Frederick Gallegos

A clear understanding of insurance and risk management is necessary to review the adequacy of an organization's DP insurance coverage. The MIS manager must be aware of the relationship between risk and insurance to understand the rationale behind insurance decisions and the types of insurance that are most applicable to the MIS environment.

Insurance distributes losses so that a devastating loss to an individual or business is spread equitably among a group of insured members. Insurance does not prevent loss nor does it reduce its costs; it merely reduces the risk. Risk is the possibility of an adverse deviation from a desired outcome (e.g., the possibility of dying before reaching age 70, a home being destroyed by fire, or an interruption in business operations).

When not managed, risks may be assumed that should be insured, and vice versa. Insurance policies often provide overlapping coverage in some areas and none in other, critical areas. Additional problems include lack of control over loss and premium costs, uneconomical insurance arrangements, organizational errors, and failure to adopt loss-prevention techniques. This chapter discusses risk management techniques, insurance alternatives, and aspects of insurance coverage.

THE REQUIREMENTS AND ADVANTAGES OF INSURANCE

The following requisites must be met for insurance companies to calculate risk in monetary terms and distribute costs over enough members to cover losses and leave a profit:[1]

- The insured objects must be of sufficient number and quantity to allow a reasonably close calculation of probable loss.
- Losses must be accidental.
- Losses must be capable of being determined and measured.
- All insured objects should not be able to be simultaneously destroyed (i.e., catastrophic hazard should be minimal).

Exhibit XI-6-1 outlines those business risks that are and are not insurable.[2]

Risks insurable commercially:

- Property risks—The uncertainty surrounding the occurrence of direct and indirect loss of property.
- Personal risks—The uncertainty surrounding the occurrence of loss of life or income as a result of:
  - —Premature death.
  - —Physical disability.
  - —Old age.
  - —Unemployment.
- Legal liability risks—The uncertainty surrounding the occurrence of loss caused by negligent behavior resulting in injury to persons arising out of:
  - —The use of automobiles.
  - —The occupancy of buildings.
  - —Employment.
  - —The manufacture of products.
  - —Professional misconduct.

Risks not insurable commercially:

- Market risks—Factors that may result in loss to property or income, including:
  - —Seasonal or cyclical price changes.
  - —Consumer indifference.
  - —Style changes.
  - —Competition offered by a better product.
- Political risks—Uncertainty surrounding the occurrence of:
  - —War or overthrow of the government.
  - —Restrictions imposed on free trade.
  - —Unreasonable or punitive taxation.
  - —Restrictions on free exchange of currencies.
- Production risks—Uncertainties surrounding occurrence of:
  - —Failure of machinery to function economically.
  - —Failure to solve technical problems.
  - —Exhaustion of raw material resources.
  - —Strikes, absenteeism, and labor unrest.

Exhibit XI-6-1. Insurable and Uninsurable Commercial Risks

Although there are obvious costs (i.e., premiums) involved in insurance, some economic and social values of insurance that may not be obvious include:[3]

- The amount of corporate accumulated funds needed to meet possible losses is reduced.
- Cash reserves that insurers accumulate are freed for investment purposes, effecting a better allocation of economic resources and increasing production.
- Because the supply of investable funds is greater than it would be without insurance, capital is available at a lower cost.
- The entrepreneur with adequate insurance coverage is a better credit risk.
- Insurers actively engage in loss-prevention activities.
- Insurance contributes to business and social stability by protecting business firms and their employees.

Insurance is an important means by which businesses can manage risk; it is not, however, the only means.

REDUCTION OF RISKS

Risks that are not insurable can be managed in other ways. By the same token, because a risk is insurable does not mean that insurance is the only way to handle it.

Risk reduction can be accomplished through loss prevention and control. If the possibility of loss can be prevented, the risk is eliminated; even reducing the chance of the loss occurring is a significant improvement. If the chances cannot be reduced, at least the severity of the loss can often be controlled. The reduction method is frequently used with insurance to lessen the premiums.

Uninsurable risks can also be reduced by risk retention, which can be voluntary or involuntary, depending on the organization's awareness of the risks. The retention method, which is sometimes referred to as self-insurance, should be voluntary and should meet the following criteria:[4]

- The risk should be spread physically so that there is a reasonably even distribution of exposure to loss over several locations.
- A study should be made to determine the maximum exposure to loss.
- Consideration should be given to the possibility of unfavorable loss experience, and a decision reached as to whether this contingency should be covered by provision for self-insurance reserves.
- A premium charge should be made against operations that is adequate to cover losses and any increase in reserves that appears advisable.

Many companies, however, retain risks without estimating the future losses or reserving funds to pay for these losses.

To decide what methods to use, companies must first analyze their risks. Managing the risk of significant losses is essential to protecting the interests of a business.

RISK MANAGEMENT

Risk management ensures that risk losses do not prevent corporate management from seeking its goals of conserving assets and maximizing profits.[5] The functions of risk management include the following:[6]

- Recognizing the exposures to loss by developing an awareness of the possibility of each type of loss. This is a basic duty that must precede all other functions.
- Estimating the frequency and size of loss by determining the probability of loss from various sources.
- Deciding the best and most economical method of managing the risk of loss, whether it be by assumption, avoidance, self-insurance, reduction of hazards, transfer, commercial insurance, or a combination of these methods.
- Administering the programs of risk management, including constant reevaluation of the programs and recordkeeping.

These functions should be carried out through the following steps:[7]

- Determining the objectives.
- Identifying the risks.
- Evaluating the risks.
- Considering the alternatives and selecting the risk treatment device.

- Implementing the decision.
- Performing an evaluation and review.

In following these steps, the organization should consider the odds and should not risk more than the company can afford to lose or risk a lot for a little.[7] These rules point out that risk management is in fact a series of cost/benefit decisions.

Determination of Objectives. A set of clearly defined objectives can guide those responsible for developing and administering the risk management program, as well as provide a means for evaluating the program's performance. Obviously, each company has objectives specifically suited to its operation; however, some broad objectives can be defined. First, the aggregate cost of risks should be kept to a minimum; in each financial year, the cost of risks should be kept below the point at which a company's assets or earnings would be significantly reduced by uninsured losses. The cost of risks is defined as the sum of the following:

- The direct and consequential costs of loss prevention measures.
- Insurance premiums.
- The cost of losses sustained (including expenses to curtail the losses).
- Net cost of indemnities from insurers and third parties.
- Expenses of relevant management, administration, and finance.

Second, the prime goals of a company should not be prejudiced. Third, a company must avoid a loss that is neither insured nor identified. Finally, the life, health, and property of others should be respected.[8] Executive management should be involved in formulating the company's risk management objectives.

Risk Identification. This step is probably the most important because unidentified risks are retained by default. Using the following identification tools can ensure a comprehensive review:[10]

- Inspection—An examination of the firm's various operation sites and discussions with managers and workers.
- Flow process chart—A flowchart of the firm's operations.
- Risk analysis questionnaire—A series of detailed questions about the company's operations.[11] If the questions are too general, unusual exposures or unique loss areas may be overlooked.
- Analysis of financial statements—An analysis of assets in the firm's balance sheet for critical areas of exposure (also referred to as asset-exposure analysis).[12] The income and expense classifications in the income statement can be similarly analyzed for areas of risk.
- Insurance policy checklist—A catalog of various policies or types of insurance that identifies insurable risks. (This information tends to ignore uninsurable risks.)

The recommended approach is to use several tools. Because each tool views the business from a different perspective, in combination they create a more complete picture of the risks to which the firm is exposed.

As a result of the increased reliance on computers and automated systems, special emphasis must be placed on the review and analysis of risks in these areas. MIS facilities and hardware are often included in the company's

overall plant and property review; however, automated systems require a separate analysis, especially when these systems are the sole source of information critical to the business. The risks associated with MIS resources include natural disasters, accidents, vandalism, and theft.[13] To assist in the identification and evaluation of MIS-related risks, the following tools and techniques have been developed:

- Security audit and field evaluation (SAFE)[14]—A checklist of risk exposures relating to data processing and a rating scale for measuring the effectiveness of the protection.
- Expected loss approach[15]—A method developed by IBM that assesses the probable loss and the frequency of occurrence for all unacceptable events for each automated system or data file. The unacceptable events are categorized as:
  - —Accidental disclosure.
  - —Deliberate disclosure.
  - —Accidental modification.
  - —Deliberate modification.
  - —Accidental destruction.
  - —Deliberate destruction.

  An algorithm is used to calculate the exposure in terms of an order of magnitude in cost.
- Scoring approach[16]—Identifies and weighs various characteristics of the automated systems. The final score is used to compare systems and rank their importance.
- ESTIMACS[17]—A software estimating system that includes certain risk-related information.
- Risk analysis and management program (RAMP)[18]—A software package developed specifically for identifying and quantifying the loss exposures related to data processing.

Risk Evaluation. Evaluation involves quantifying or ranking the size and probability of a potential loss. The risks can then be categorized as follows:[19]

- Critical—All exposures in which the possible losses are of a magnitude that would result in bankruptcy.
- Important—Those exposures in which the possible losses would not lead to bankruptcy but would require the firm to take out loans to continue operations.
- Unimportant—Those exposures in which the possible losses could be accommodated by existing assets or current income without imposing undue financial strain.

Assigning the identified risks to one of these categories gives it a level of significance and helps in determining the proper means for treating it.

Choice of Techniques. Risks can be managed using one of the following techniques:

- Avoidance.
- Prevention.
- Reduction.

1. High severity or catastrophic loss risks:
   - Why is the loss so severe?
   - How will the loss arise?
   - What are the shortcomings of the existing control procedures?
2. Avoidance:
   - Is it impossible to avoid?
   - Is it impractical to avoid?
   - Is it too expensive to avoid?
   - Is it too time-consuming to avoid?
3. Prevention:
   - Are there any direct countermeasures to prevent the risk from occurring?
   - Are they cost-effective?
   - Do they have beneficial side effects?
   - Do they have adverse side effects?
4. Reduction:
   - Are there any direct countermeasures to reduce the risk?
   - Are they cost-effective?
   - Do they reduce the loss occurrence?
   - Will other risks be reduced as well?
   - Do they have beneficial side effects?
   - Do they have adverse side effects?
5. Transfer:
   - By insurance?
   - By contractual agreement?
   - By other means?
   - Are there other benefits?
   - Can the risk be best dealt with by a combination of controls?
   - Can it be partially reduced and partially transferred?
   - What are the benefits of each method?
6. Retention:
   - By self-insurance?
   - By other means?
   - Can it be partially reduced and partially retained?
   - What are the benefits of each method?

Exhibit XI-6-2. Risk Exposure Techniques Checklist

- Transfer
- Retention.

More than one technique may be applied to a given risk (as is usually the case with reduction and transfer or retention). The risk management objectives should be used as a guide in choosing a technique. As list of questions to consider when selecting a technique is provided in Exhibit XI-6-2.[20] If consideration is being given to the transfer technique and, in particular, the use of insurance, the following additional items should be taken into account:[21]

- Advantages of deductibles—Retaining a portion of the risk (i.e., the deductible) can greatly reduce insurance costs (i.e., premiums).
- Tax considerations—The impact of tax laws on insurance costs and losses may influence the decision. In business, property and liability insurance premiums are a deductible expense, as are uninsured losses. Contributions to a funded retention program are not deductible.

- Selection of the insurer—Factors to consider in selecting an insurer include:[22]
  - —Availability of coverage.
  - —Cost of coverage.
  - —Financial solvency, stability, and profitability of the insurer.
  - —Quantity and quality of service offered, both by the insurer directly and through the agency system that it uses.

If consideration is being given to retaining the risks, the following major financial aspects must be analyzed in assessing the value of the loss retention:[23]

- Cash flow—Because losses are not always paid for when they occur, a company may have the use of those funds for varying periods and may earn a return on them until such time as the losses are actually paid.
- Opportunity cost of funds—If a fund is set up to meet losses, the firm may experience some loss in interest that could be earned if the money were used in the business as working capital.

In general, the financial advantage of loss retention is greater when:[24]

- The difference is small between interest rates on liquid accounts and rates of return on capital employed within the business.
- Commercial insurance rates on the risk are relatively high compared with the opportunity costs of funds.
- The firm's perceived needs for liquid loss reserve funds are low (i.e., the firm becomes more willing to accept risks).

Finally, the records and documents of past losses and risk decisions can be used as a prime information source in the process of choosing the appropriate risk-handling technique. In this way, the knowledge, experience, and patterns of the past can be put to good use.

Once the appropriate technique has been chosen, it must be implemented. The necessary facts and figures are now available to help negotiate insurance, set up a loss-prevention program, or establish a loss-reserve fund. Exhibit XI-6-3 illustrates the risk analysis structure up to this point.[25] The various implemented plans must now be evaluated and reviewed. This is an important process because the variables are constantly changing (e.g., new risks arise, old ones disappear, and techniques that were appropriate last year may not be this year) and mistakes sometimes occur; the wrong technique or the wrong coverage must be detected before it proves too costly.[26]

DETERMINING ADEQUATE DP INSURANCE COVERAGE

Risk management functions act as a guide during the review of DP insurance coverage. It first must be understood why insurance was selected. The steps outlined in the previous section can help verify that:

- The objectives of the risk management policy are in line with the overall goals of the organization.
- The methods used to identify the risks associated with data processing provide an accurate and comprehensive list.
- Risk exposures are properly quantified and categorized.
- The appropriate decision has been made after consideration of the alternatives.

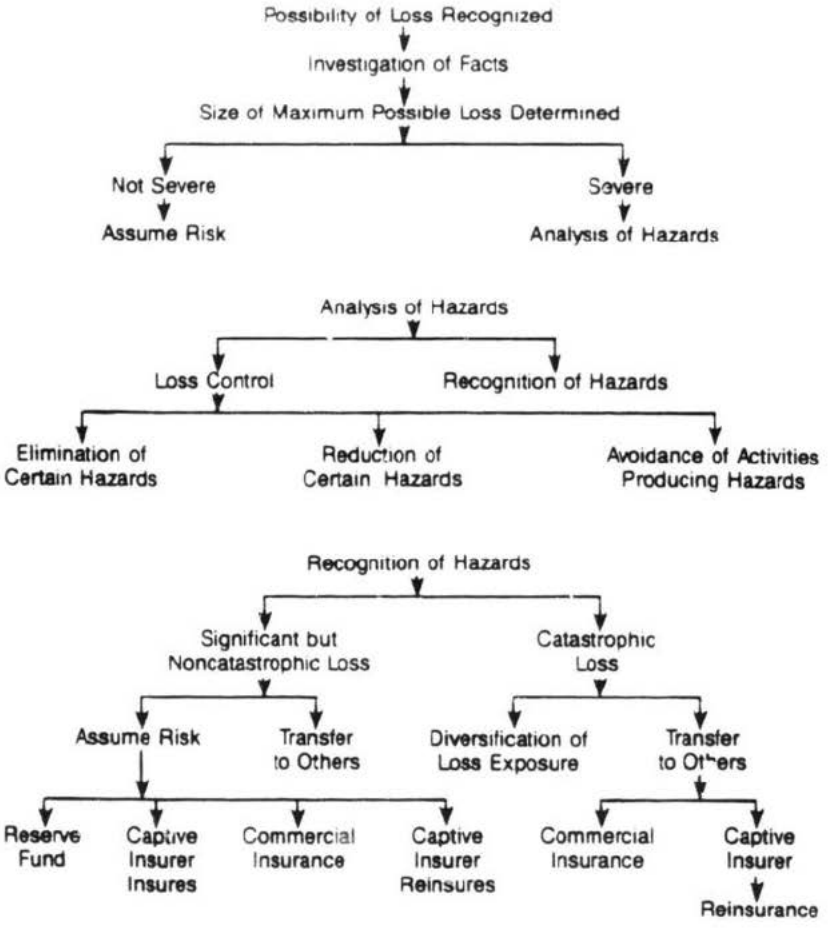

Exhibit XI-6-3. Structure of Risk Analysis

After the risk management process has been reviewed, a more detailed investigation of MIS-related risks can commence. The following is a list of questions that must be addressed:

- Prevention and reduction:
  - —Is there a comprehensive, up-to-date disaster recovery/contingency plan?
  - —What efforts have been made to check that the plan is workable?
  - —Are the backup and retention of critical files adequate?
  - —Are there off-site backups of the appropriate files?
  - —Are the procedures and practices for controlling accidents adequate?
  - —Have practical measures been taken to control the impact of a disaster?
  - —Is physical security adequate to protect property and equipment?

  - —Is software security adequate to protect important or sensitive information?
  - —Are there appropriate balancing and control checks made at key points in the processing?
  - —Are there appropriate control checks on the operations?
  - —Are there appropriate control checks during the development and modification of systems?
  - —Do contracts for purchases or leases have terms and conditions that adequately protect the company if there is a problem?
  - —Are facilities and equipment maintained properly?
- Transfer:
  - —Are those risks that should be handled by insurance, according to the risk management objectives and the risk analysis, in fact being done so?
  - —Has the insurer been evaluated?
- Retention:
  - —Are risks retained that, according to the risk management objectives and the risk analysis, should be?
  - —Have deductibles been used judiciously in insurance policies?

Once the methods available to prevent and reduce risk losses have been examined and the risks to be insured have been determined, attention can be focused on the insured risks.

In the MIS environment, there are special risks that are commonly handled by insurance, including:[27]

- Damage to the computer equipment.
- Cost of storage media.
- Cost of acquiring the data stored on the media.
- Damage to outsiders.
- Business effects of the loss of computer functions.

The types of insurance policies that cover these risks include property, liability, business interruption, and fidelity-bonding insurance. Exhibit XI-6-4 provides a checklist for a review program that deals with insurance coverage.[28]

The review of the policies specially written for MIS-related risks should examine:[29]

- Coverage of hardware and equipment (i.e., tape drives, terminals, printers, and CPUs).
- Coverage of media and information stored thereon—For example, a blank tape that is destroyed can be replaced at the cost of a blank tape. If the tape contains important information, however, the value of the tape plus the value of the lost information must be recovered.
- Coverage of the replacement or reconstruction cost and the cost of doing business as usual (i.e., business interruption)—This might involve renting time on equivalent equipment from a nearby company, paying overtime wages for reconstruction, and "detective work."
- Noncoverage of such items as damage to media from magnets, damage from power failure (blackout) or power cut (brownout), and damage from software failure.

1. Secure and examine statements of company policy covering insurance.
2. Review written procedures, memorandums, and other material to determine whether:
   - Instructions covering the procurement and maintenance of coverage in accordance with company policy are in force.
   - Procedures are adequate for personnel.
3. Review contract files, lease files, and pertinent risk analyses to determine whether the risk management department is informed of risks to which the company may be exposed, so that adequate coverage may be maintained in accordance with company policy.
4. Determine requirements for company insurance coverage under loan agreements, sales contracts, and similar items. Verify that the requirements are met.
5. Determine whether responsibility for informing the risk management department of contracts and contract revisions is assigned and enforced so that adequate coverage may be maintained.
6. Prepare a schedule of policies in force with outside carriers showing:
   - Coverage.
   - Exposure.
   - Locations.
   - Premium.
   - Other pertinent data.
7. Review the types and limits of coverage. Make sure that they are maintained in general accordance with company policy.
8. Examine policies and related correspondence to verify that:
   - Policies on file are listed in the schedule and policies on the schedule are on file.
   - Policies are adequately safeguarded.
   - All significant data is shown on the schedule.
   - The company is shown as the insured.
   - Where applicable, subsidiary divisions, locations, and companies are specified.
   - Endorsements are physically attached to policies and are properly applicable.
   - Required premiums or deposits are appraised for reasonableness and accuracy.
   - Risks and exclusions or restrictions are definitely specified and are applicable.
9. Review and test the procedures followed by the risk management department to ensure that:
   - When orders for insurance are placed, binders and policies are received.
   - Renewal of policies is adequately controlled.
   - Policies are considered for renewal in sufficient time to permit consideration of changes.
   - Invoices for premiums and deposits are reviewed and approved by the risk management department before forwarding to accounts payable for payment.
   - Financial position of insurance carriers is checked periodically.
10. Secure a copy of any reports rendered to management on insurance operations and check any financial figures shown on reports with appropriate original records. These reports should cover:
    - Premium cost.
    - Insurable values.
    - Claims paid.
    - Savings made.

Exhibit XI-6-4. Insurance Review Checklist

After it has been verified that the proper items are covered in the policies, the dollar values assigned must be checked. The risk analysis data gathered during the evaluation step of the risk management process should be used to compare the dollar values in the policies with the quantified risk exposures. This comparision, however, must take into account any prevention or reduction actions as well as any retained risks (e.g., as with deductibles).

SUMMARY

Organizations must develop a sound risk management program in order to determine the adequacy of their DP insurance coverage. The first step in

properly developing a program is becoming aware of the limits and advantages of insurance and learning the methods of risk reduction. For the risk management program itself, objectives must be determined; risks must be identified, categorized, and evaluated; and risk-handling techniques must be chosen. Understanding insurance choices and the types of policies available is also important.

The development of a comprehensive risk management program is a long process and a lot of work. Once established, however, the benefits become invaluable.

Notes

1. M.R. Greene and J.S. Trieschmann, *Risk and Insurance* (Cincinnati: South-Western Publishing Co, 1981), p 21.
2. Greene and Trieschmann, p 23.
3. E.J. Vaughan and C.M. Elliott, *Fundamentals of Risk and Insurance* (New York: John Wiley & Sons Inc, 1978), p 27.
4. B. Cadmus, *Operational Auditing Handbook* (Orlando FL: The Institute of Internal Auditors, 1964), p 427.
5. Vaughan and Elliott, p 30.
6. Greene and Trieschmann, pp 34–35.
7. Vaughan and Elliott, p 35.
8. Vaughan and Elliott, p 35.
9. W.K. Fallon, ed, *AMA Management Handbook* (New York: American Management Associations Inc, 1983), pp 11–15.
10. Vaughan and Elliott, pp 32–33.
11. B.J. Daenzer, *Fact-Finding Techniques in Risk Analysis* (New York: American Management Associations Inc, 1970), pp 39–60.
12. Daenzer, pp 63–67.
13. H. Schaeffer, *Data Center Operations* (Englewood Cliffs NJ: Prentice-Hall Inc, 1981), p 126.
14. L.I. Kraus, *SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems* (East Brunswick NJ: Firebrand, Kraus, & Co Inc, 1972).
15. R.M. Leung, "Risk Assessment of EDP Systems" (Masters Project, California State Polytechnic University, Pomona, 1983), pp 15–16.
16. Leung, pp 22–23.
17. F.A. Scheigel, Jr, "ESTIMACS Summary" (Valley Forge PA: Management and Computer Services Inc, 1984), pp 2–3.
18. R.V. Jacobson, "A Practical Data Processing Risk Analysis Methodology" (New York: International Security Technology Inc, 1980), pp 1–11.
19. Vaughan and Elliott, p 34.
20. K.K. Wong, *Risk Analysis and Control* (Rochelle Park NJ: NCC Publications and Hayden Book Co Inc, 1970), pp 114–115.
21. Vaughan and Elliott, pp 41–42.
22. Greene and Trieschmann, p 110.
23. Greene and Trieschmann, pp 41–42.
24. Greene and Trieschmann, p 42.
25. Greene and Trieschmann, p 44.
26. Vaughan and Elliott, p 35.
27. W.C. Mair, D.R. Wood, and K.W. Davis, *Computer Control and Audit* (New York: Touche Ross & Co, 1978), p 352.
28. Cadmus, pp 438–440.
29. J. Martin, *Security, Accuracy, and Privacy in Computer Systems* (Englewood Cliffs NJ: Prentice-Hall Inc, 1973), pp 581–582.