MANAGEMENT OBJECTIVE

Identify, analyze, and manage risk in a way that both controls the entity's present and potential losses and meets the entity's goals and objectives.

Return to Table of Contents

BACKGROUND

Every entity is exposed to risk (loss). The dynamic and changing nature of an entity's operating environment itself generates risks that could adversely affect financial, physical, information, and human resources. Such seemingly routine occurrences as staff turnover, new services development, or legislative change can create risks.

Some of these risks, such as the risk that client populations will significantly increase, can have a material impact on an entity's ability to provide services. Other risks, such as the risk of not having enough pencils in stock, are not important enough to be worth managing. Once the material risks are identified, management must determine the probability that a given loss will occur and then select the decision alternative most likely to avoid such loss.

The fact that management must base these decisions on incomplete information also creates risk. "There is no correct choice among the various criteria for making decisions. The decision ultimately depends on the individuals' value systems as well as society's. It is crucial that decision frameworks be carefully chosen and that the choices be derived both logically and consistently, particularly in complex situations" (Morgan, p. 40). See the module on problem-solving and decision-making for more information.

No practical way exists to reduce risk to zero. Management must determine and maintain the level of risk it deems prudent. The approach to this task must be ongoing, disciplined, coordinated, and acknowledged. However, management must also consider the costs associated with the risk management process. Some risks may cost more to manage than the cost of the actual loss to be avoided.

Risk assessment can occur as a free-standing process. It can also be found within many management processes. The strategic planning process, for example, usually includes a scan of the environment to identify changes that may put the entity at risk. The regulatory process in state government includes an assessment of the risk to the public created by certain industry operating practices. Regulatory agencies, such as the Banking Department, are then established. These agencies design their auditing and monitoring functions to minimize these risks.

DEFINITIONS

Risk includes:

- any event which could adversely affect the entity
- the degree to which activities are exposed to:
  - financial loss
  - the inappropriate disclosure of data
  - ineffective use of human resources
- the tendency of a system or function to have problems
- the potential for negative consequences

Risk avoidance is not engaging in activity that would produce a loss.

Risk exposure is the possibility of loss or injury.

Risk management is the process used to identify, analyze, and control risk in order to minimize present and potential loss to an entity. Risk management is an ongoing iterative process. Identifying and managing risk is an important component of an effective internal control system.

- **Risk identification** is the process of determining which losses could negatively affect the entity's ability to fulfill its goals and objectives.
- **Risk analysis** is the process of determining both the probability of the occurrence of loss and the potential impact of such occurrence.
- **Risk control** is the process of choosing a method for eliminating or controlling the negative impact of the identified risk.

Risk prevention is making changes to keep a loss from occurring.

Risk reduction is reducing the severity of loss when it occurs.

Rules, as used in this module, are the criteria management uses to assess risk. Such rules can be based on rights, technology, or utility (Morgan, pp. 37-38).

- **Rights-based rules** are concerned with justice. In rights-based systems, there are certain things one party cannot do to another without its consent, regardless of costs and benefits. Legal sanctions against crime are examples of risk control based upon rights.
- **Technology-based rules** are concerned with the level of technology available to control certain risks. In technology-based systems, costs, benefits, and rights assume secondary importance in risk control. National defense, counterintelligence, and home security are possible examples of risk control systems based on technology.
- **Utility-based rules** are concerned with the trade-offs between costs and benefits. Since risk management can require significant investments, costs of risk control must be weighed against benefits, e.g., should the entity hire one more security guard or one more administrative technician?

OVERVIEW OF THE PROCESS

The basic phases of a risk assessment process are (Texas Workers' Compensation Commission, Vol. I, Chap. 2, p. 1):

- **Identify the risk.**
- **Assess the significance of the risk.**
- **Select an appropriate method of managing the risk.**
- **Implement the appropriate method.**
- **Evaluate the method application/program.**

PROCEDURES

Suggested procedures, organized according to the elements of a finding, are listed below. They should be expanded or tailored to fit the specific entity being reviewed. Since risk assessment is likely to be a part of other processes, how it should be approached will depend a great deal upon the process it is supporting.

In general, an entity's approach to managing risk is likely to be more informal and intuitive than the process outlined here suggests. The process outline should be used only as a guide, not as a checklist of steps that the entity must have. The ultimate test of whether the process used by the entity is appropriate will be whether or not it works. You should not recommend changes to the existing process unless there is evidence of real identified problems and/or risks.

Review Criteria:
General Criteria

General criteria applicable to the risk assessment process are as follows:
Risk assessment has three primary objectives:

- Identify, analyze, and act upon risks which might hamper achievement of the entity's objectives.
- Identify those risks with higher potential for adverse affects.
- Determine the priority of risk to be addressed with limited resources.

Specific Criteria

The criteria related to the basic phases of the risk assessment process are as follows:

Identify the risk

Risk identification can be vital to entity success. Unidentified risk can greatly affect achievement of goals and objectives. Thus, identifying risk is best integrated with the planning process, and risks associated with entity goals and objectives should be closely considered.

Risk identification should be ongoing. Since risk identification is only a snapshot of risk exposure, it must be continuous to capture all elements of change within an entity over a period of time (Texas Workers' Compensation Commission, Vol. I, Chap. 3, p. 1).

Risk identification should be sufficiently thorough to specify risks associated with significant interactions between funds, people, goods, services, and information and between the entity and relevant external factors. In other words, the entity should identify the resources (funds, people, goods, services, and information) that are needed for continued operation and think about what could impair its ability to obtain these resources when needed.

Entities should focus risk identification on both internal and external environments. External factors may include technological developments, new regulation or legislation, and economic changes. For example, a significant change in the market interest rate could negatively affect the ability of a retirement fund to control its rate of return on investments. Internal factors include changes in management responsibilities, an unassertive or ineffective board, or lack of qualified personnel (Committee of Sponsoring Organizations of the Treadway Commission, p. 92).

Whether or not a particular factor constitutes a risk will depend on the entity. Weather is an important risk factor for the road crews in the Department of Transportation. It would not be an important risk factor for the State Auditor's Office.

Assess the significance of the risk

Risk analysis should include determination of both the probability of the occurrence of loss and the actual or potential fiscal impact of the loss to the entity (Texas Workers' Compensation Commission, Vol. I, Chap. 4, p. 1).

To adequately assess significance, entities should formally quantify risk or exposure to loss, e.g., via actuarial projections, failure mode and effect analysis, fault tree analysis, or other decision analysis technique(s) (see Problem-Solving and Decision-Making: Appendix). Frequency and severity of loss should be tracked over time since such trends provide a way to budget for current and future losses (Texas Workers' Compensation Commission, Vol. I, Chap. 4, p. 1 and "Risk Ranking" in *The Hub*, p. 1-C-20).

Select an appropriate method of managing the risk

Management should determine how best to manage the risk by identifying necessary actions and related controls. Specifically, management should address whether or not the negative impact of a present or potential risk can and/or should be eliminated or controlled.

Management must be clear about the rules it uses to determine whether to deal with a particular risk and then devote resources toward eliminating or controlling the risk. The three basic categories of rules are rights-based, technology-based, and utility-based (Morgan, p. 38).

The following methods can be used to control risk (Texas Workers' Compensation Commission, Vol. I, Chap. 5, pp. 1-2):

- Eliminate or avoid the risk by not undertaking the activity that produces the risk.
  - Example: A state agency requires that payments from customers be made by check to avoid the risks associated with handling cash.
- Prevent the risk by educating the participants or altering the situation that produces the risk.
  - Example: A state agency conducts training on sexual harassment to prevent the risk of loss due to inappropriate employee behavior.
- Reduce the risk by adding procedures that assume the risk is not avoidable but act to minimize the loss.
  - Example: Sprinklers are required in office buildings to reduce the damage caused by fires.
- Reduce the risk by separating or diversifying the exposure or having backup ready in case of loss.
  - Example: A board sets up investment policies that require the diversification of investments.
- Transfer the financial and/or legal liabilities associated with the risk outside the entity.
  - Example: An agency elects to lease, as opposed to buy a building.

If risks are material, and cannot be controlled by one of these methods, management should identify ways to finance the cost of the loss. For example, the entity could set up reserves to pay for the loss or purchase insurance to cover the loss (Texas Workers' Compensation Commission, Vol. I, Chap. 6, pp. 1-2).

Implement the appropriate method

Effective implementation of risk elimination and control methods requires the knowledge, participation, and cooperation of managers and employees. Managers and affected employees should be involved in management's decisions regarding allocation of entity resources to effect the risk method (Texas Workers' Compensation Commission, Vol. I, Chap. 2, p. 2).

Evaluate the method application/program

Entities should review their risk assessment processes to ensure continued efficiency and effectiveness. In so doing, information should be gathered at all levels of the entity engaged in risk assessment activity. Risk assessment systems should be examined in the context of entity plans to ensure continued alignment with entity goals and objectives. The cost effectiveness of entity risk assessment efforts should also be periodically examined.

Risk assessment systems should be sensitive to changes in the operating environment, organizational structure and function, client needs, and turnover in staff or assets. Any such system should be flexible enough to implement changes should it vary from its expected course (Texas Workers' Compensation Commission, Vol. I, Chap. 2, p. 2).

Assess Condition:

Determine the actual processes used

Conduct interviews, observe operations, and identify and collect available documentation in order to gain an understanding of the entity's actual risk assessment process and controls. Included in the actual process are both official/unofficial and formal/informal processes and controls. An official process may exist even if it is not documented. Possible procedures include, but are not limited to:

- Determine how the entity plans for ongoing risk assessment and the relationship between such plans and the entity's strategic plan.
- Identify the material risk areas for the process/function/program being reviewed. Determine how risk is managed within the process/function/program.
- Obtain and review documentation of how risk assessment works within that process, including policies, procedures, manuals, forms, annual reports, and risk assessment reports.
- Determine whether or not risk assessment includes risk identification, risk analysis, and risk management.
- Determine the rules management uses for risk assessment.
- Determine the techniques management uses for risk avoidance, risk prevention, and risk reduction.
- Determine how the entity assesses and addresses the frequency of identical or similar losses.
- Determine how the entity assesses and addresses the severity (size or cost) of losses.
- Determine what sort of risk assessment information is routinely maintained in entity files.
- Identify and establish the functions and relationships of entity personnel involved in the allocation and expenditure of resources devoted to risk assessment.
- Interview appropriate employees about the frequency, nature, and scope of risk assessment activities.
- Determine how the entity communicates risk information to the various participants in the risk assessment system.
- Determine how management benchmarks, measures, evaluates, and documents the performance of the risk assessment system.

In addition to gaining an understanding of the actual process, also try to find out:

- how the participants view their own process
- what they think is important about the process, and why

This information may help identify causes and barriers.

Determine the strengths and weaknesses of the actual process

Using the tailored criteria, the understanding of the entity's process gained above, and the procedures in this section, analyze the actual process to determine if it:

- is designed to accomplish the management objective (this module, page 1)
- has controls that provide reasonable assurance that the process will work as intended
- is implemented and functioning as designed
- is actually achieving the desired management objective(s)

In executing these procedures, remember to identify and analyze both strengths and weaknesses.

Identify and review the steps in the actual process. Possible procedures include, but are not limited to:

- Determine if all major steps in the criteria are included in the actual process. If steps are missing, determine if they are likely to have a material impact on the process.
- Determine if all the steps in the process appear to add value. If there are steps that do not appear to add value, try to get additional information on why they are included in the process.
- Review the order of the steps in the process to determine if it promotes productivity.
- Review the level of technology used in the process to determine if it is up-to-date and appropriate to the task. (Besides computer, electronic, communications and other technology, this may include management and decision-making technology, e.g. actuarial projections, failure mode and effect analysis, fault tree analysis, and other decision analysis tools).

Identify the controls over the process and determine if the controls are appropriate, placed at the right point(s) in the process, timely, and cost effective. Possible procedures include, but are not limited to:

- Draw a picture of the process, the controls, and the control objectives (see the graphic of the procurement process in the Introduction for an example). Determine if the control objectives are in alignment with the overall management objective(s). Flowcharts of the risk assessment process can help identify inputs, processes, and outputs, as well as the critical elements of an entity's operations.
- Examine the nature, scope, and effectiveness of the controls used to ensure that risk assessment is ongoing, thorough, and timely. (If controls are at the end of the process, they may not be as effective in ensuring ongoing, thorough, and timely risk assessment).
- Determine how management reviews risk assessment system performance to ensure maintenance of standards and minimization of risk. Determine how such standards are benchmarked and compared to actual performance, and whether such standards are measurable, quantifiable, and both task and results-oriented. For example, if a

regulatory entity has a monitoring function that uses a risk assessment process to determine how it handles complaints, does it review the outcome of the process to determine if it actually identifies and resolves the highest risk complaints first?

- Determine how management changes the risk assessment process if either performance standards and goals or entity objectives are not met.
- Identify, describe, and assess the process used to gather input from employees who might reasonably discover flaws in the risk assessment system.

Review observations, interviews, documentation and other evidence and design specific audit procedures as needed to determine if the process and/or the controls are functioning as designed. Depending upon the objectives of the project, these procedures may include both tests of controls and substantive tests. Possible procedures include, but are not limited to:

- Establish how information on the risk assessment system, its implementation, and its results are communicated to appropriate staff.
- Determine whether appraisals of the risk assessment system are done as frequently as formally stated in entity policy and/or as advised by good management practice.

Analyze process reports over time for trends. Determine whether the information gained from the monitoring process is fed back AND is used to modify the system. Possible procedures include, but are not limited to:

- Review the results of evaluations of the risk assessment process. Determine the extent to which such information is used to refine risk assessment needs and enhance the capabilities and performance of the risk assessment process.

Determine causes

Determine what circumstances, if any, caused the identified weaknesses in the risk assessment process. Possible procedures include, but are not limited to:

- Determine if the participants in the risk assessment process understand its relationship to the entity's mission, goals, and values.
- Determine if the participants understand their role in the risk assessment process.
- If the process occurs at multiple locations, determine the nature and scope of communication and coordination between them.
- Determine if the relationship between the risk assessment process and other entity processes is clear.
- Determine if the risk assessment process has adequate human, dollar, time, and asset resources.
- If there are negative trends in the monitoring reports, determine if the reports are communicated to and used by the appropriate parties.

Determine what internal or external constraints or barriers, if any, must be removed in order to successfully overcome these weaknesses. Possible procedures include, but are not limited to:

- Determine if any key employees are unwilling to change the process and why they are unwilling.
- Review the applicable entity, state or federal laws or regulations to determine if any of them prevent the necessary changes from being made in the process.

Determine effect

Determine the effect of each of the weaknesses identified in terms of dollars, impact on services (either quantity or quality), impact on citizens, impact on the economy, etc. Possible procedures include, but are not limited to:

- Identify benchmarks for the process in question and compare to actual performance. Quantify the difference, if possible.
- Estimate the cost before and after the proposed change and compare.
- Estimate the quantity and/or quality of services before and after the proposed change and compare.
- Identify the risks associated with not making the proposed change and quantify.

Develop recommendations

Use the tailored criteria, references in the resource section, the identified weaknesses, and the identified causes and barriers to develop specific recommendations to address the cause and correct the weaknesses. Possible procedures include, but are not limited to:

- Identify alternative solutions used by other entities.
- Identify solutions for removing barriers.
- Provide general guidelines as to the objectives each solution should meet. Then the entity can tailor the solution to its specific situation.
- Provide specific information, if available, on how each recommendation can be implemented.

RESOURCES

Articles

Morgan, M. Granger. "Risk Analysis and Management." *Scientific American* 269:1:32-41, July 1993. Location: Methodology Project Information Resources Folders.

Books

Committee of Sponsoring Organizations of the Treadway Commission. *Internal Control: Integrated Framework -- Executive Summary, Revised Draft.* New York, NY: Committee of Sponsoring Organizations of the Treadway Commission, February 1992. Location: Methodology Project Information Resources Folders.

Committee of Sponsoring Organizations of the Treadway Commission. *Internal Control: Integrated Framework -- Exposure Draft.* New York, NY: Committee of Sponsoring Organizations of the Treadway Commission, March, 1991. Location: Methodology Project Information Resources Folders.

Texas Workers' Compensation Commission, Risk Management Division. *Risk Management for Texas State Agencies.* Volume I, *Risk Management Administration.* Austin, TX: Texas Workers' Compensation Commission, August 16, 1991. Location: Methodology Project Information Resources Folders.

Data Bases

A search of the UTCAT on-line data base at the University of Texas' Perry-Castañeda Library reveals the following:

- risk assessment
  - 197 books
  - 136 articles in academic periodicals
  - 115 articles in business periodicals
- risk management
  - 285 books
  - 99 articles in academic periodicals
  - 1539 articles in business periodicals

Note: Do a TK (title keyword) search in UTCAT to find books. Do a PK (periodical keyword) search in the academic or business periodical index to find articles.

Human Resources

The following SAO staff members have specialized training or ongoing interest in risk assessment:

Employee	Title/Function
Jarrett Oliver Johanna Peavy, CPA Tony Rose, CPA	Regulatory Effectiveness Project Team

Babette Laibovitz, MPA Linda Lansdowne, CPA Sheila McNaney Bruce Truitt	Module Writers/Editors
Barbara Hankins, CPA Jeannie Henderson, CPA Randy Townsend, CPA	Reviewers

Periodicals

Journal of Risk and Insurance
Published by the American Risk and Insurance Association
Location: The University of Texas, Perry-Castañeda Library (368.05 J827)

National Underwriter Property and Casualty - Risk and Benefits Management
Published weekly by the National Underwriter Company
Location: The University of Texas, Perry-Castañeda Library (MFICHE 8944)

Risk Analysis
Published quarterly by the Society for Risk Analysis and Plenum Publishing
Location: The University of Texas, Perry-Castañeda Library (T 174.5 R55)

Risk Management
Published monthly by the Risk and Insurance Management Society
Location: The University of Texas, Perry-Castañeda Library (HG 8059 C7 N312)

Professional Associations

American Risk and Insurance Association
Bloomington, Illinois
(309) 454-6900

Risk and Insurance Management Society
New York, New York
(212) 286-9292

Society for Risk Analysis
8000 Westpark Drive, Suite 130
McClean, Virginia 22102
(
703) 790-1745 (703) 790-9063 FAX

Related Modules and Reports

SAO internal report: *Regulatory Effectiveness Model*