General Security Risk Assessment

GUIDELINE

ASIS INTERNATIONAL
Advancing Security Worldwide™

ASIS INTERNATIONAL GUIDELINES COMMISSION

The ASIS International Guidelines Commission was established in early 2001 by ASIS International (ASIS) in response to a concerted need for guidelines regarding security issues in the United States. As the preeminent organization for security professionals worldwide, ASIS has an important role to play in helping the private sector protect business and critical infrastructure from terrorist attacks. Whereas ASIS previously had chosen not to promulgate guidelines and standards, the events of 9/11 brought to the forefront the need for a professional security organization to spearhead this initiative. By addressing specific concerns and issues inherent to the security industry, security guidelines will better serve the needs of security professionals by increasing the effectiveness and productivity of security practices and solutions, as well as enhance the professionalism of the industry.

Mission Statement of the ASIS Guidelines Commission

To advance the practice of security through the development of risk mitigation guidelines within a voluntary, non-proprietary, and consensus-based process utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership and the security industry.

Goals and Objectives

- Assemble and categorize a database of existing security-related guidelines
- Involve/organize ASIS Councils to support guidelines
- Develop and sustain alliances with related organizations
- Develop methodology for identifying recommended guidelines
- Identify and develop methodology for development, documentation, and acceptance of guidelines
- Produce national consensus-based guidelines in cooperation with other industries and the Security Industry Standards Council

Functions

- Assignment of guideline committee(s)
- Approve membership on guideline committees(s)
- Determine/select guidelines for development and assign scope
- Establish guideline projects to develop security guidelines
- Act as a correlating body to effectively manage and integrate guidelines from various ASIS Councils and security disciplines
- Monitor, revise, and update ASIS' Glossary of Terms
- Review and monitor projects and project guideline development
- Approve Final Draft Guidelines
- Adjudicate appeals
- Select guidelines for submission to the Security Industry Standards Council for accreditation as American National Standards

An ASIS International Guideline

GENERAL SECURITY RISK ASSESSMENT

ASIS INTERNATIONAL GUIDELINES COMMISSION

Published by ASIS International
Alexandria, Virginia

© ASIS International. All rights reserved.
1625 Prince Street, Alexandria, Virginia 22314-2818 USA
703-519-6200

I. Title

The title of this guideline is *The General Security Risk Assessment Guideline.*

II. Revision History

November 13, 2002 Guideline approved

III. Commission Members

Sean Ahrens, CPP
Norman Bates
Chad Callaghan, CPP
Pamela Collins, EdD, CFE
Grant Crabtree, CPP
Michael Crane, CPP
Edward Flynn, CFE
Arthur Kingsbury, CPP
Michael Stack
Basil Steele, CPP
Don Walker, CPP
Timothy Walsh, CPP
Timothy Williams, CPP

IV. Keywords

Risk, Assessment, Vulnerability, Threat, Asset, Security Survey

V. Guidelines Designation

This guideline is designated as ASIS GLCO 01 012003.

VI. Scope

This guideline is applicable in any environment where people and/or assets are at risk for a security-related incident or event that may result in human death, injury, or loss of an asset.

VII. Summary of Guideline

The General Security Risk Assessment seven-step process creates a methodology for security professionals by which security risks at a specific location can be identified and communicated, along with appropriate solutions. The guideline also includes definitions of terms, a process flow chart, illustrative material in appendices, and references/bibliography.

VIII. Purpose

To provide a methodology for security professionals by which security risks at a specific location can be identified and communicated, along with appropriate solutions.

IX. Terminology

Assets
Any real or personal property, tangible or intangible, that a company or individual owns that can be given or assigned a monetary value. Intangible property includes things such as goodwill, proprietary information, and related property. For purposes of this guideline, people are included as assets.

Consequential
A secondary result ensuing from an action or decision. From an insurance or security standpoint, costs, loss, or damage beyond the market value of the asset lost or damaged, including other indirect costs.

Cost/Benefit Analysis
A process in planning, related to the decision to commit funds or assets. This is a systematic attempt to measure or analyze the value of all the benefits that accrue from a particular expenditure. Usually, this process involves three steps:

- Identification of all direct and indirect consequences of the expenditure.
- Assignment of a monetary value to all costs and benefits resulting from the expenditure.
- Discounting expected future costs and revenues accruing from the expenditure to express those costs and revenues in current monetary values.

Criticality
The impact of a loss event, typically calculated as the net cost of that event. Impact can range from *fatal,* resulting in a total recapitalization, abandonment, or long-term discontinuance of the enterprise, to *relatively unimportant.*

Events
Something that happens; a noteworthy happening. In the security context, this usually represents an occurrence such as a security incident, alarm, medical emergency, or related episode or experience.

Goodwill
The value of a business that has been built up through the reputation of the business concern and its owners.

Loss Event
An occurrence that actually produces a financial loss or negative impact on assets. Examples include security incidents, crimes, war, natural hazards, or disasters.

Natural Disaster
A naturally occurring calamitous event bringing great damage, loss, or destruction such as tornadoes, hurricanes, earthquakes, and related occurrences.

Copyright © 2003 ASIS International

Probability
The chance, or in some cases, the mathematical certainty that a given event will occur; the ratio of the number of outcomes in an exhaustive set of equally likely outcomes that produce a given event to the total number of possible outcomes.

Qualitative
Relating to that which is characteristic of something and which makes it what it is.

Quantitative
Relating to, concerning, or based on the amount or number of something, capable of being measured or expressed in numerical terms.

Risk
The possibility of loss resulting from a threat, security incident, or event.

Risk Analysis
A detailed examination including risk assessment, risk evaluation, and risk management alternatives, performed to understand the nature of unwanted, negative consequences to human life, health, property, or the environment; an analytical process to provide information regarding undesirable events; the process of quantification of the probabilities and expected consequences for identified risks.

Risk Assessment
The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel.

Security Incident
A security-related occurrence or action likely to lead to death, injury, or monetary loss. An assault against an employee, customer, or supplier on company property would be one example of a security incident.

Security Vulnerability
An exploitable capability; an exploitable security weakness or deficiency at a facility, entity, venue, or of a person.

Site
A spatial location that can be designated by longitude and latitude.

State-of-the-Art
The most advanced level of knowledge and technology currently achieved in any field at any given time.

Statistics
A branch of mathematics dealing with the collection, analysis, interpretation, and presentation of masses of numerical data. In security, this could represent a collection of quantitative data such as

security incidents, crime reports, and related information that, together with other like information, serves as security-related statistics used for a number of applications including risk and vulnerability evaluations.

Threat

An intent of damage or injury; an indication of something impending.

X. Recommended Practice Advisory

Practice advisories provide the security practitioner with guidance regarding the application of specific security processes. They support and provide interpretation for this and future guidelines. Additional practice advisories on the same or similar topics may be developed by or submitted to the ASIS International Guidelines Commission (Commission) to address a variety of special circumstances that include different industries, geographical areas, information technology, and related applications. The following steps describe the Commission's recommended approach and framework for conducting *General Security Risk Assessments*:

1. **Understand the organization and identify the people and assets at risk**. *Assets* include people, all types of property, core business, networks, and information. *People* include employees, tenants, guests, vendors, visitors, and others directly or indirectly connected or involved with an enterprise. *Property* includes tangible assets such as cash and other valuables and intangible assets such as intellectual property and causes of action. *Core business* includes the primary business or endeavor of an enterprise, including its reputation and goodwill. *Networks* include all systems, infrastructures, and equipment associated with data, telecommunications, and computer processing assets. *Information* includes various types of proprietary data.

2. **Specify loss risk events/vulnerabilities.** Risks or threats are those incidents likely to occur at a site, either due to a history of such events or circumstances in the local environment. They also can be based on the intrinsic value of assets housed or present at a facility or event. A loss risk event can be determined through a vulnerability analysis. The vulnerability analysis should take into consideration anything that could be taken advantage of to carry out a threat. This process should highlight points of weakness and assist in the construction of a framework for subsequent analysis and countermeasures.

3. **Establish the probability of loss risk and frequency of events**. *Frequency of events* relates to the regularity of the loss event. For example, if the threat is the assault of patrons at a shopping mall, the frequency would be the number of times the event occurs each day that the mall is open. *Probability of loss risk* is a concept based upon considerations of such issues as prior incidents, trends, warnings, or threats, and such events occurring at the enterprise.

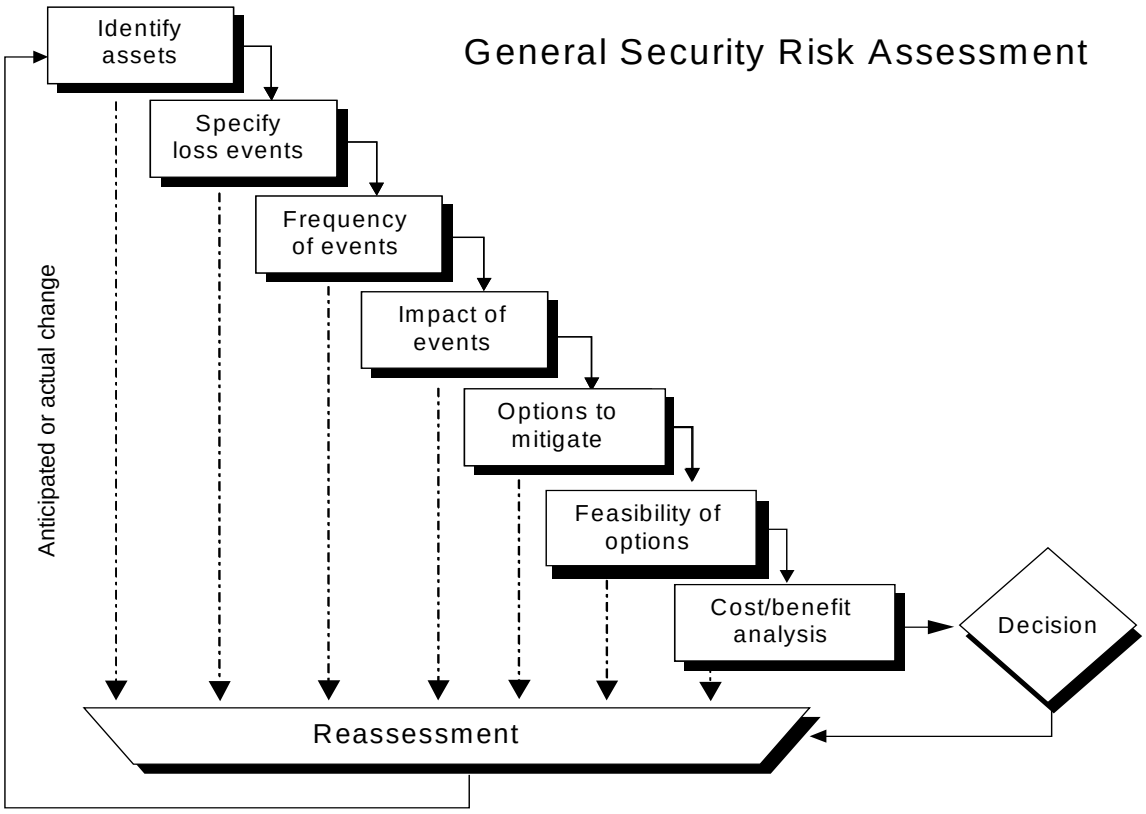
4. **Determine the impact of the events**. The financial, psychological, and related costs associated with the loss of tangible or intangible assets of an organization.

5. **Develop options to mitigate risks**. Identify options available to prevent or mitigate losses through physical, procedural, logical, or related security processes.

6. **Study the feasibility of implementation of options**. Practicality of implementing the options without substantially interfering with the operation or profitability of the enterprise.

7. **Perform a cost/benefit analysis**. See definition in section IX. Terminology.

Copyright © 2003 ASIS International



Process Flow Chart. This flow chart graphically represents this process.

XI. Information Sources for Determining Loss Risk Events

1. Local police crime statistics
2. Uniform Crime Reports (UCR) or comparable data
3. Organization internal documents (e.g., security incident reports)
4. Prior complaints from employees, customers, guests, visitors, etc.
5. Prior civil claims for inadequate security
6. Intelligence from local, state, or national law enforcement agencies about potential threats
7. Industry-related information about trends
8. General economic conditions of the area
9. Presence of a crime magnet (e.g., proximity of a popular night club, continuous presence of vagrants, property in disrepair)

XII. References/Bibliography

The process of evaluating the risk of crime at a specific location or geographical area is widely recognized and has been adopted nationwide by private industry, public law enforcement, municipalities, and other governmental agencies. The following published sources reference the process used to perform a crime risk analysis. This list is not all-inclusive but is a representative sampling of available references.

"American Society for Testing & Materials - Draft Standard Guide for Determining Design Criteria for the Physical Protection of a Facility," American Society for Testing & Materials, Philadelphia, PA, August 1996.

Apo, Allan. "Security for Apartment Buildings." *Crime Prevention Report* no. 93.10. (1991): 3-4.

Apo, Allan. "Security for Parking Facilities." *Crime Prevention Report* no. 93.40. (1992): 1-2.

Bates, Norman D. "Security Experts Preparation of Plaintiff & Defense Cases." *Negligent Security Cases,* 1993.

Bates, Norman D. *Premises Liability for the Criminal Acts of Third Parties*. Massachusetts Bar Association Continuing Legal Education, April 1996.

Bellmio, Peter. "Crime Analysis and Crime Prevention," chap. 34. In *Handbook of Loss Prevention and Crime Prevention, 2nd Ed.* ed. Lawrence J. Fennelly. Boston: Butterworths, 1989.

Biery, Ken D. Jr., and James L. Schaub. *The Ultimate Security Survey*. Boston, MA: Butterworth-Heinemann, 1994.

Broder, James F. *Risk Analysis and the Security Survey*. Boston, MA: Butterworth-Heinemann, 1984.

Bursik, Robert J. Jr. *Neighborhoods and Crime*. New York, NY: Lexington Books, 1993.

Chuda, Thomas J. *Basic Crime Prevention Curriculum*. International Society of Crime Prevention Practitioners. Columbus, OH: 1990.

Crowe, Timothy D. *Crime Prevention Through Environmental Design*. Boston, MA: Butterworth-Heinemann, 1991.

D'Addario, Francis James. *Loss Prevention through Crime Analysis*. Boston, MA: Butterworths, 1989.

Department of the Navy, Naval Facilities Engineering Command. *Physical Security Design Manual 13.1*. Washington, DC: Government Printing Office, 1983.

Fennelly, Lawrence J. *Effective Physical Security: Design, Equipment, and Operations*. Boston, MA: Butterworth-Heinemann, 1992.

Fennelly, Lawrence J. *Handbook of Loss Prevention and Crime Prevention, 3rd Ed.* Boston, MA: Butterworth-Heinemann, 1996.

Fennelly, Lawrence J. *Handbook of Loss Prevention and Crime Prevention, 2nd Ed.* Boston, MA: Butterworths, 1989.

Floyd, William R. *Security Surveys: Guidelines for Evaluating*, Crete, IL: Abbott, Langer & Associates, 1995.

Garcia, Mary Lynn, *The Design and Evaluation of Physical Protection Systems*. Boston, MA: Butterworth-Heinemann, 2001.

Girard, Charles M. "Planning, Management and Evaluation," chap.31. In *Handbook of Loss Prevention and Crime Prevention, 2nd Ed.* Ed. Lawrence J. Fennelly. Boston, MA: Butterworths, 1989.

Green, Gion, and revised by Robert J. Fischer. *Introduction to Security, 4th Ed.* Boston, MA: Butterworths, 1987.

"Guide Being Developed for Determining Design Criteria for Physical Protection of a Facility." *ASTM Standardization News*. August 1996.

Harold, Victor. "Site Survey and Risk Assessment," chap 4. In *Effective Physical Security: Design, Equipment and Operations*. Boston, MA: Butterworth-Heinemann, 1992.

Healy, Richard J. and Timothy J. Walsh. *Protection of Assets Manual*. Los Angeles, CA: POA Publishing, LLC, 2002.

Imwinkelreid, Edward J. "Admissibility of Nonscientific Expert Testimony." *TRIAL,* October 1996, vol. 32, #10.

Lyons, Stanley L. *Security of Premises: A Manual for Managers*. London: Butterworths, 1988.

McNamee, David, *Business Risk Assessment*, Altamonte Springs, FL: Institute of Internal Auditors, 1998.

McGoey, Chris E. *Security Adequate…or Not?* Oakland, CA: Aegis Books, 1990.

Morrison, Mahoney & Miller. *Defending the Negligent Security Claim*. Boston, MA. 1992.

 Copyright © 2003 ASIS International

National Crime Prevention Council. *350 Tested Strategies to Prevent Crime.* Washington, D.C., National Crime Prevention Council, 1995.

National Crime Prevention Institute. "Designing Crime Risk Management Systems," chap. 38. In *Handbook of Loss Prevention and Crime Prevention, 3rd Ed.* Ed. Lawrence J. Fennelly. Boston, MA: Butterworth-Heinemann, 1996.

National Crime Prevention Institute. *Understanding Crime Prevention.* Boston, MA: Butterworths, 1986.

National Governors Association. *Kids & Violence.* Ed. Linda McCart. Washington, D.C., National Governors Association, 1994.

Peltier, Thomas, *Information Security Risk Analysis*, Boca Raton, FL: Auerbach/CRC Press, 2001.

Post, Richard S. and Kingsbury, Arthur A. *Security Administration: An Introduction, 3rd Ed.* Springfield, IL: Charles C. Thomas, 1977.

Purpura, Philip P. *Security and Loss Prevention: An Introduction, 2nd Ed.* Boston, MA: Butterworth-Heinemann, 1991.

Roper, Carl A. *Risk Management for Security Professionals*, Boston, MA: Butterworth-Heinemann, 1999.

Sennewald, Charles A. *Effective Security Management, 2nd Ed.* Boston, MA: Butterworth Publishers, 1985.

Sherman, Lawrence W. "Violent Stranger Crime at a Large Hotel: A Case Study in Risk Assessment Methods." *Security Journal*, Vol. 1, No. 1 (1989): 40-46. Stoneham, MA: Butterworth Publishers.

U.S. Army Corps of Engineers. *Security Engineering Manual.* January 1990. Missouri River Division/Omaha District.

U.S. Department of Justice, U.S. Marshals Service. *Vulnerability Assessment of Federal Facilities.* Washington, D.C.: Government Printing Office, 1995.

U.S. Department of Justice, Federal Bureau of Investigation. *Crime in the United States, 1995, Uniform Crime Reports.* Washington, D.C.: U.S. Government Printing Office, 1996.

Waldhuber, Robert M. "Assessing Security Needs," pp. 12-15. In *Security and Safety: Issues and Ideas for Shopping Center Professionals.* New York, NY: International Council of Shopping Centers, 1989.

XIII. Appendices

I. Qualitative Approach: Suggested Approach, Methodology, and Sources of Information
II. Quantitative Approach: Calculating Probability and Criticality

XIV. Commentary

The ASIS International Guidelines Commission is comprised of representatives from many of the major security organizations in the United States and is fortunate for the wealth of experience in the field that they bring to the table. The Commission will soon assume a role of strategic coordination and planning. For this initial guideline, however, the Commission produced the document without the assistance of any subcommittee or other group. After the initial draft was completed in the summer of 2002, select leaders of ASIS councils and committees reviewed the document. The second draft went to a much broader population of security professionals who submitted numerous comments back to the Commission. The Commission then reviewed and evaluated each comment and made changes, additions, and modifications where necessary. The resulting document attempts to bring the concepts of risk assessment to the widest audience possible and therefore is written in the most general terms.

APPENDICES

Suggested Approach, Methodology, and Sources of Information

The purpose of these appendices are to provide explanatory material to illustrate, by example, the type of approach, methodology, and sources of information, as well as the options for consideration by the security professional when a security risk assessment is conducted. It is recognized that, in some cases, the data available regarding one or more security risks may be too sparse to permit a thorough quantitative assessment. In such cases, a qualitative approach should be used based upon the seven-step model shown.

The appendices are intended to provide the user a series of examples for illustrative purposes only. They are neither required, recommended, mandated courses of action, nor prescribed methodologies. The practitioner should use whatever information, technology, or other resources may assist in the Security Risk Assessment process.

Copyright © 2003 ASIS International

APPENDIX I: Qualitative Approach

Each step of the following seven-step practice advisory includes examples and other relevant information to guide the practitioner in developing a better understanding of the underlying principles to be applied in the assessment.

PRACTICE ADVISORY #1

Understand the organization and identify the people and assets at risk.

COMMENTARY - "Understand the organization"

The first task of the security practitioner is to develop an understanding of the organization to be assessed. This does not mean that the practitioner must become an expert in the operation of the enterprise to be evaluated, but must acquire enough of an understanding of how the organization operates to appreciate its complexities and nuances. Consideration should be of factors such as hours of operation; types of clients served; nature of the business activity; types of services provided or products produced, manufactured, stored, or otherwise supplied; the competitive nature of the industry; the sensitivity of information; the corporate culture; the perception of risk tolerance; and so on.

The types of information that the practitioner should ascertain:

- The hours of operation for each department
- Staffing levels during each shift
- Types of services provided and/or goods produced, stored, manufactured, etc.
- Type of clientele served (e.g., wealthy, children, foreigners, etc.)
- The competitive nature of the enterprise
- Any special issues raised by the manufacturing process (e.g., environmental waste, disposal of defective goods, etc.)
- Type of labor (e.g., labor union, unskilled, use of temporary workers, use of immigrants, etc.)

COMMENTARY - "Identify the people and assets at risk"

The second step in the process is to identify the assets of the organization that are at risk to a variety of hazards.

People

People include employees, customers, visitors, vendors, patients, guests, passengers, tenants, contract employees, and any other persons who are lawfully present on the property being assessed. In very limited circumstances, people who are considered trespassers also may be at risk for open and obvious hazards on a property or where an attractive nuisance exists (e.g., abandoned warehouse, vacant building, a "cut through" or path routinely used by people to pass across property as a short cut). In most states, trespassers need only be warned by the posting of signs of a known dangerous or hazardous condition.

Property

Property includes real estate, land and buildings, facilities; tangible property such as cash, precious metals, and stones; dangerous instruments (e.g., explosive materials, weapons, etc.); high theft items (e.g., drugs, securities, cash, etc.); as well as almost anything that can be stolen, damaged, or otherwise adversely affected by a risk event.

Property also includes the "goodwill" or reputation of an enterprise that could be harmed by a loss risk event. For example, the ability of an enterprise to attract customers could be adversely affected by a reputation as being unsafe or crime ridden.

The third subset of property is information. Information includes proprietary data, such as trade secrets, marketing plans, business expansion plans, plant closings, confidential personal information about employees, customer lists, and other data that if stolen, altered, or destroyed could cause harm to the organization.

PRACTICE ADVISORY #2

Specify loss risk events/vulnerabilities.

COMMENTARY

The second major step in the security risk assessment methodology is to identify the types of events or incidents which could occur at a site based on the history of previous events/incidents at that site; events at similarly situated sites; the occurrence of events (e.g., crimes) that may be common to that type of business; natural disasters peculiar to a certain geographical location; or other circumstances, recent developments, or trends.

Loss risk events can fall into three distinct categories: crimes, non-criminal events such as human-made or natural disasters, and consequential events caused by an enterprise's relationship with another organization, when the latter organization's poor or negative reputation adversely affects the enterprise.

SOURCES OF DATA AND INFORMATION

Crime-Related Events

There are numerous sources for information/data about crime-related events that may impact an enterprise. The security practitioner may consider any of the following sources in aiding the determination of risk at a given location.

- Local police crime statistics and calls for service at the site and the immediate vicinity for a three-to-five year period
- Uniform Crime Reports published by the U.S. Department of Justice for the municipality
- The enterprise's internal records of prior reported criminal activity
- Demographic/social condition data providing information about economic conditions, population densities, transience of the population, unemployment rates, etc.
- Prior criminal and civil complaints brought against the enterprise
- Intelligence from local, state, or federal law enforcement agencies regarding threats or conditions that may affect the enterprise
- Professional groups and associations that share data and other information about industry-specific problems or trends in criminal activity
- Other environmental factors such as climate, site accessibility, and presence of "crime magnets"

Non-Criminal Events

The practitioners should consider two subcategories of non-crime-related events: natural and "human-made" disasters. Natural disasters are such events as hurricanes, tornadoes, major storms, earthquakes, tidal waves, lightning strikes, and fires caused by natural disasters. "Human-made" disasters or events could include labor strikes, airplane crashes, vessel collisions, nuclear power plant leaks, terrorist acts (which also may be criminal-related events), electrical power failures, and depletion of essential resources.

Copyright © 2003 ASIS International

Consequential Events

A "consequential" event is one where, through a relationship between events or between an enterprise and another organization, the enterprise suffers some type of loss as a consequence of that event or affiliation, or when the event or the activities of one organization damage the reputation of the other. For example, if one organization engages in illegal activity or produces a harmful product, the so-called innocent enterprise may find its reputation tainted by virtue of the affiliation alone, without any separate wrongdoing on the part of the latter organization.

PRACTICE ADVISORY # 3

Establish the probability of loss risk and frequency of events.

COMMENTARY - Probability of Loss Risk

Probability of loss is not based upon mathematical certainty; it is consideration of the likelihood that a loss risk event may occur in the future, based upon historical data at the site, the history of like events at similar enterprises, the nature of the neighborhood, immediate vicinity, overall geographical location, political and social conditions, and changes in the economy, as well as other factors that may affect probability.

For example, an enterprise located in a flood zone or coastal area may have a higher probability for flooding and hurricanes than an enterprise located inland and away from water. Even if a flood or hurricane has not occurred previously, the risks are higher when the location lends itself to the potential for this type of a loss risk event.

In another example, a business that has a history of criminal activity both at and around its property will likely have a greater probability of future crime if no steps are taken to improve security measures and all other factors remain relatively constant (e.g., economic, social, political issues).

The degree of probability will affect the decision-making process in determining the appropriate solution to be applied to the potential exposure.

COMMENTARY - Frequency of events

When looked at from the "event" perspective, the practitioner may want to query how often an exposure exists per event type. For example, if the event is robbery of customers in the parking lot, then the relevant inquiry may be how often customers are in the lot and for how long when walking to and from their vehicles. If the event is the rape of a resident in an apartment building, then the inquiry may focus on how often the vulnerable population is at risk. If the event were a natural disaster such as a hurricane, the practitioner certainly would want to know when hurricane season takes place.

PRACTICE ADVISORY #4

Determine the impact of the event.

COMMENTARY

The security practitioner should consider all the potential costs, direct and indirect, financial, psychological, and other hidden or less obvious ways in which a loss risk event impacts an enterprise. Even if the probability of loss is low, but the impact costs are high, security solutions still are necessary to manage the risk.

Direct costs may include:

- Financial losses associated with the event, such as the value of goods lost or stolen
- Increased insurance premiums for several years after a major loss
- Deductible expenses on insurance coverage
- Lost business from an immediate post-risk event (e.g., stolen goods cannot be sold to consumers)
- Labor expenses incurred as a result of the event (e.g., increase in security coverage post event)
- Management time dealing with the disaster/event (e.g., dealing with the media)
- Punitive damages awards not covered by ordinary insurance

Indirect costs may include:

- Negative media coverage
- Long-term negative consumer perception (e.g., that a certain business location is unsafe)
- Additional public relations costs to overcome poor image problems
- Lack of insurance coverage due to a higher risk category
- Higher wages needed to attract future employees because of negative perceptions about the enterprise
- Shareholder derivative suits for mismanagement
- Poor employee morale, leading to work stoppages, higher turnover, etc.

PRACTICE ADVISORY # 5

Develop options to mitigate risks.

COMMENTARY

The security practitioner will have a range of options available, at least in theory, to address the types of loss risk events faced by an enterprise. "In theory" alludes to the fact that some options may not be available either because they are not feasible (discussed in Practice Advisory #6) or are too costly, financially or otherwise.

Options include security measures available to reduce the risk of the event. Equipment or hardware, policies and procedures, management practices, and staffing are the general categories of security-related options. However, there are other options, including transferring the financial risk of loss through insurance coverage or contract terms (e.g., indemnification clauses in security services contracts), or simply accepting the risk as a cost of doing business.

Any strategy or option chosen still must be evaluated in terms of availability, affordability, and feasibility of application to the enterprise's operation.

Copyright © 2003 ASIS International

PRACTICE ADVISORY #6

Study the feasibility of implementation of options.

COMMENTARY

The practical considerations of each option or strategy should be taken into account at this stage of the security risk assessment. While financial cost is often a factor, one of the more common considerations is whether the strategy will interfere substantially with the operation of the enterprise. For example, retail stores suffer varying degrees of loss from the shoplifting of goods. One possible "strategy" could be to close the store and keep out the shoplifters. In this simple example, such a solution is not feasible because the store also would be keeping out legitimate customers and would go out of business.

In a less obvious example, an enterprise that is open to the public increases its access control policies and procedures so severely that a negative environment is created by effectively discouraging people from going to that facility as potential customers and hence, loses business.

The challenge for the security practitioner is to find that balance between a sound security strategy and consideration of the operational needs of the enterprise, as well as the psychological impact on the people affected by the security program.

PRACTICE ADVISORY # 7

Perform a cost/benefit analysis.

COMMENTARY

The final step in conducting a security risk analysis is consideration of the cost versus benefit of a given security strategy. The security practitioner should determine what the actual costs are of the implementation of a program and weigh those costs against the impact of the loss, financially or otherwise. For example, it would make no sense to spend $100,000 on security equipment to prevent the theft of a $1,000 item, especially when it may make more sense to purchase insurance or remove the item to a more secure location.

APPENDIX II: Quantitative Approach

CALCULATING PROBABILITY AND CRITICALITY

LOSS EVENT PROFILE

Forecasting individual loss events that may occur is the first step in dealing with risk assessment. It requires clear ideas about the kinds of loss events or risks, as well as about the conditions, circumstances, objects, activities, and relationships that can produce them. A security countermeasure can be planned if the loss event has the following characteristics:

- The event will produce an actual loss, measurable in some standard medium, such as money; and
- The loss is not the result of a speculative risk in that nonoccurrence of the event would not result in a gain.

The kinds of events that are loss-only oriented and which involve so called "pure risks" include crime, natural catastrophe, industrial disaster, civil disturbance, war or insurrection, terrorism, accident, conflicts of interest, and maliciously willful or negligent personal conduct. The recognition of even obvious risks implies some estimate of the probability that the risk actually will produce a loss. To the extent that the risk itself is concealed, the task of estimating probability of occurrence is more difficult.

LOSS EVENT PROBABILITY OR FREQUENCY

Probability can be formulated as the number of ways in which a particular event can result from a large number of experiments which could produce that event, divided by the number of those experiments. Stated as an equation, this is:

$$P = \frac{f}{n}$$

where:

P = the probability that a given event will occur
f = the number of actual occurrences of that event
n = the total number of experiments seeking that event

E.g., the probability of shoplifting at a given location during a given year is determined as: *p* (probability) = the number of days on which actual shoplifting events occurred during the year divided by 365. Although this simple statement illustrates a direct way to calculate probability mathematically, it is not enough for practical application to security loss situations, because while some events will occur more than once, other events will occur only once, and the reaction will so change the environment that the theoretically probable further occurrences will be prevented. As a basic concept, *the more ways a particular event can occur in given circumstances, the greater the probability that it will occur*. For effective assessment of probability, as many as possible of those circumstances that could produce the loss must be known and recognized.

Copyright © 2003 ASIS International

Probability Factors

Conditions and sets of conditions that will worsen or increase asset exposure to risk of loss can be divided into the following major categories:

1. *Physical environment* (construction, location, composition, configuration)
2. *Social environment* (demographics, population dynamics)
3. *Political environment* (type and stability of government, local law enforcement resources
4. *Historical experience* (type and frequency of prior loss events)
5. *Procedures and processes* (how the asset is used, stored, secured)
6. *Criminal state-of-art* (type and effectiveness of tools of aggression)

Application of Probability Factors Analyses

The practical value of loss risk analysis depends upon the skill and thoroughness with which the basic risks to an enterprise are identified. This is the first and most important step in the entire process. Every aspect of the enterprise or facility under review must be examined to isolate those conditions, activities, and relationships that can produce a loss. For an effective analysis, the observer must take into account the dynamic nature of the enterprise on each shift and between daylight and darkness. The daily routine must be understood, because the loss-producing causes can vary from hour to hour.

Checklists

Every enterprise differs from every other, and general recommendations must be modified to meet local needs. Consult the references in this guideline for forms and checklists to use in the initial gathering of loss event data.

RISK MATRIX

After analysis has identified the specific threats or risks, the details that make occurrence of each event more or less probable can be recorded. The method suggested is a grid or matrix arranged either by asset or by type of risk, setting forth all the factual elements relevant to probability. Matrices describe a particular situation with respect to each of the risks identified in the general fact gathering. Please see Figure 1, infra. The frequent absence or scarcity of historical occurrence data often makes it impossible to calculate probability on a purely quantitative basis and requires some degree of qualitative assessment.

Asset Identification and Description

CONDITIONS AFFECTING RISK

LOCATION	Value ($)	Admittance Controlled (Y/N)	Area Locked (Y/N)	Records Kept (Y/N)	Alarms (Y/N)	Other →
Warehouse						Etc.
Front Office						Etc.
Laboratory						Etc.
Shipping						Etc.
Manufacturing						Etc.
Etc.						Etc.

Figure 1. Specimen Matrix. Locations and Conditions Affecting Risk can be added and/or modified to fit the particular asset and its environment. (Y/N) = Yes or No for each condition specified. Conditions should be framed such that a Yes indicates better and a No indicates poorer protection.

Probability Ratings

After all the available data concerning each risk and its factual circumstances have been gathered, a probability rating can be assigned to that risk. Ratings will not consider any precaution or countermeasure that may later be taken to reduce or eliminate the risk. A primary purpose of such unconditioned ratings is to allow for later priority scheduling in the selection of countermeasures. It may be enough to be able to say one event is more probable than another. To say this about entire series or categories of events, it must be possible to assign each to some class that can then be compared with other classes to arrive at a conclusion of "more likely" or "less likely." Five categories of probability can establish useful distinctions among events, as follows:

(A) Virtually Certain — Given no changes, the event will occur. For example, given no changes, a closed intake valve on a sprinkler riser will prevent water flow in event of fire.
(B) Highly Probable — The likelihood of occurrence is much greater than that of nonoccurrence. For example, unprotected currency lying visible on a counter is very likely to be taken.
(C) Moderately Probable — The event is more likely to occur than not to occur.
(D) Less Probable — The event is less likely to occur than not to occur. This does not imply impossibility, merely improbability.
(E) Probability Unknown — Insufficient data are available for an evaluation.

This approximate system of ratings contains wide latitude for variation. Two observers could assign different probabilities to the same risk, based upon different evaluations of the circumstances. But an advantage of this technique is that absolute precision is not important. If the correct general label can be attached, it doesn't matter that a highly probable risk might have a ratio of .751 or .853. What is important is to be able to segregate all risks of virtually certain probability from all others, and to make similar distinctions for each other general class. Even competent professionals may disagree on what is highly probable and what is moderately probable. To compensate for inexactness, if a rating is in doubt after all available information has been gathered and evaluated, then the higher of two possible ratings should be assigned.

Rating Symbols. To save time and space, five levels of probability can be assigned the symbols **A, B, C, D,** and **E**, ranking downward from "Virtually Certain" to "Probability Unknown." These symbols later will be combined with symbols representing criticality in the development of priority lists. It should be noted that the probability rating **E**, or "Probability Unknown," is merely a temporary rating pending the development of all relevant data. In the construction of threat logic patterns, **E** ratings will be replaced by one of the definite ratings.

The second step in risk analysis is complete when a particular risk, identified in the first level of the survey through the use of forms and checklists, has been assigned a probability rating. No standard recording system is in universal use and each protection organization making a survey must set up its own recording system to be sure that each risk, once identified, can be found readily again in the growing volume of survey data. A simple method for doing this is to assign a distinctive number to each risk classified. It will be necessary to locate and identify each risk to add a later criticality rating, to rank the rated risk in a table or priority list, and to plot it in a threat logic tree based on relative priorities.

Copyright © 2003 ASIS International

LOSS EVENT CRITICALITY

Highly probable risks may not require countermeasures attention if the net damage they would produce is small. But even moderately probable risks require attention if the size of the loss they could produce is great. The correlative of probability of occurrence is severity or criticality of occurrence. Assessing criticality is the third step in risk assessment. Criticality is first considered on a single event or occurrence basis. For events with established frequency or high recurrence probability, criticality also must be considered cumulatively. The criticality or loss impact can be measured in a variety of ways. One is effect on employee morale; another is effect on community relations. But the most useful measure overall is financial cost. Because the money measure is common to all ventures, even government and not-for-profit enterprises, the seriousness of security vulnerability can be grasped most easily if stated in monetary terms.

Note that some losses, e.g.. loss of human life, loss of national infrastructure elements, or losses of community goodwill, do not lend themselves to ready analysis in financial terms. When events that could produce these types of losses have been identified, some factors other than merely quantitative will be used to measure their seriousness.

When tradeoff decisions are being made as part of the risk management process, a very useful way to evaluate security countermeasures is to compare cost of estimated losses with cost of protection. Money is the necessary medium.

Kinds of Costs to Be Considered

Costs of security losses are both direct and indirect. They are measured in terms of lost assets and lost income. Frequently, a single loss will result in both kinds.

.

1. Permanent Replacement

The most obvious cost is that involved in the permanent replacement of a lost asset. Permanent replacement of a lost asset includes all of the cost to return it to its former location. Components of that cost are: 1. *Purchase price* or *manufacturing cost*; 2. *Freight and shipping charges*; and 3. *Make-ready or preparation cost to install it or make it functional*. A lost asset may cost more or less to replace now than when it was first acquired.

2. Temporary Substitute

It may be necessary to procure substitutes while awaiting permanent replacements. This may be necessary to minimize lost opportunities and to avoid penalties and forfeitures. The cost of the temporary substitute is properly allocable to the security event that caused the loss of the asset. Components of temporary substitute cost might be: 1. *Lease or rental*; and/or 2. *Premium labor*, such as overtime or extra shift work to compensate for the missing production.

3. Related or Consequent Cost

If other personnel or equipment are idle or underutilized because of the absence of an asset lost through a security incident, the cost of the downtime also is attributable to the loss event.

4. Lost Income Cost

In most private enterprises, cash reserves are held to the minimum necessary for short-term operations. Remaining capital or surplus is invested in varying kinds of income-producing securities. If cash that might otherwise be so invested must be used to procure permanent replacements or temporary substitutes or to pay consequent costs, the income that might have been earned must be considered part of the loss. If income from investment is not relevant to a given case, then alternative uses of the cash might have to be abandoned to meet the emergency needs. In either case, the use of the money for loss replacement will represent an additional cost margin. To measure total loss impact accurately, this also must be included. The following formula can be used:

$$I = \frac{P \times r \times t}{365}$$

where:
I = income earned
P = principal amount (in dollars) available for investment
r = annual per cent rate of return
t = time (in days) during which P is available for investment

Cost Abatement

Many losses are covered, at least in part, by insurance or indemnity of some kind. To the extent it is available, that amount should be subtracted from the combined costs of loss enumerated previously.

A Cost-of-Loss Formula

Taking the worst-case position and analyzing each security loss risk in light of the probable maximum loss for a single occurrence of the risk event, the following equation can be used to state that cost:

$$K = Cp + Ct + Cr + Ci) - I$$

where:
K = criticality, total cost of loss
Cp = cost of permanent replacement
Ct = cost of temporary substitute
Cr = total related costs
Ci = lost income cost
I = available insurance or indemnity

Criticality Ratings

It is suggested that the following ratings be used to summarize the impact of each loss event, and interpreted as follows:

1. **Fatal** — The loss would result in total recapitalization or abandonment or long-term discontinuance of the enterprise.
2. **Very serious** — The loss would require a major change in investment policy and would have a major impact on the balance sheet assets.

Copyright © 2003 ASIS International

3. **Moderately serious** — The loss would have a noticeable impact on earnings as reflected in the operating statement and would require attention from the senior executive management.
4. **Relatively unimportant** — The loss would be charged to normal operating expenses for the period in which sustained.
5. **Seriousness unknown** — Before priorities are established, this provisional rating is to be replaced by a firm rating from one of the first four classes.

The nature and size of the enterprise determines the dollar limits for each of these classes. The value of the rating system is in its relevance to the enterprise. The terms used are not intended to have any absolute significance. This completes the third step in vulnerability assessment.

ALTERNATIVE APPROACHES TO CRITICALITY

Known Frequency Rate

There are other ways in which the weighted importance of a probable risk event can be measured. One is when a historical frequency can be identified. For example, natural catastrophes such as floods and earthquakes are expected to occur a stated number of times per year, based upon the number of actual past occurrences. Other events also may have a reliable rate of recurrence. When a frequency rate is known, the single event criticality can be multiplied by the number of events expected during the period considered, normally the calendar or fiscal year. Thus, if K = $10,000 for an event, and it has a frequency rate of once a year, the weighted impact would be $10,000 x 1. If the same event had a frequency rate of once every three years, the weighted impact would be $10,000 x .333 or $3,333. If it had a frequency of three times a year, the weighted impact would be $10,000 x 3 or $30,000.

Nominal Numerical Probability

Another technique, useful to convert the symbolic rankings to simple numerical statements, is to assign an agreed real numerical probability to each of four categories below. Thus: A) "Virtually Certain", might be assigned a numerical probability of .85; B) "Highly Probable" might be assigned .65; C) "Moderately Probable" might be assigned .50; and D) "Less Probable" might be assigned .20.

Next, the criticality of any single loss event is multiplied by the agreed value of the probability. Thus, a $10,000 criticality for a moderately probable event would be $10,000 x .50 = $5,000. (Note that this is used hypothetically to arrive at an overall picture of exposure. If the loss occurs at all, it will cost $10,000, not $5,000.) But to permit ranking before loss so as to expedite countermeasures, the technique would preserve the weighted differences.

Scatter Plots

Another method to present overall risk is to use a scatter plot. This is a method of plotting each risk on a graph whose axes are cost and frequency. First, the criticality or cost impact is located on the vertical axis. Then, moving right in a straight line, a dot or mark is placed above the frequency rate for that event on the horizontal axis. When all the risks have been plotted on the graph, a smooth curve (a line passing through the areas of highest concentration of dots) can be drawn. This would indicate the approximate distribution of expected losses for the planning period. The countermeasures program would be designed to lower that line as much as feasible. See Figure 2, infra.

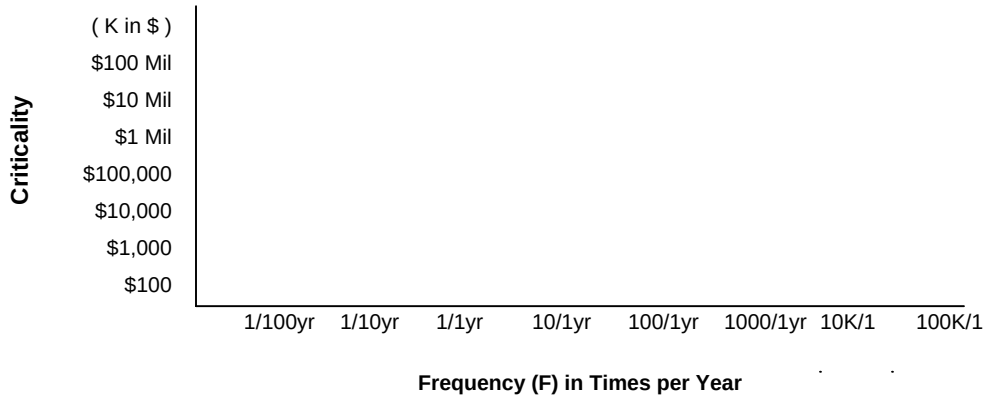


Figure 2. Specimen scatter plot; to show events weighted for Criticality (K) (Vertical Axis) and Frequency (times per year)(horizontal axis). Each event or risk is plotted at the intersection of K and F for that event.

Establishing Priorities

The next step is to arrange the entire body of rated risks into a sequence of priority for countermeasures attention. The more serious risks are listed first, followed in descending order of importance by the others until all the risks have been listed. The listing should identify each risk and indicate the combined probability-criticality rating that has been assigned. Such an approach would produce a list of all the risks in each of the various rating classes, as follows: A1, A2, A3, A4; B1, B2, B3, B4; C1, C2, C3, C4; D1, D2, D3, D4.

When the risks have all been ranked, the formal task of risk assessment is complete and reflects the risk exposure of the enterprise as of the date on which the assessment was made. No risk assessment is permanent and, depending upon the extent and speed of changes within the enterprise, reassessments will be required periodically, at a minimum of at least once a year.

Copyright © 2003 ASIS International

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 32,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, governmental entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine — *Security Management* — ASIS leads the way for advanced and improved security performance.

Advancing Security Worldwide™

1625 Prince Street
Alexandria, VA 22314-2818 USA
703-519-6200
Fax: 703-519-6299
www.asisonline.org