

FUNDAMENTALS OF HEALTH CARE RISK MANAGEMENT

I. INTRODUCTION TO HEALTH CARE RISK MANAGEMENT

- A. Historical overview
 - 1. Acute- hospital based concept
 - 2. Acute- outpatient/ambulatory concept
 - 3. Networks
- B. Scope
 - 1. Protect the financial assets
 - 2. Promote organizational goals and objectives
- C. Definitions
 - 1. Risk finance
 - a. Risk analysis
 - b. Risk acceptance
 - c. Risk avoidance
 - 2. Claims management
 - 3. Clinical risk management
 - a. Risk analysis
 - b. Risk reduction
 - 4. Risk prevention

II. RISK MANAGEMENT PROCESS

- A. Why?
 - 1. Promotes quality
 - 2. Protects assets
 - 3. Prevents injury
- B. What?
 - 1. Identification and assessment of risk
 - 2. Analysis of findings
 - 3. Treatment through control and/or financing
 - 4. Evaluation
 - 5. Reassessment

III. RISK ASSESSMENT

- A. Industry risk assessments
 - 1. Closed claims trends nationally/regionally
 - 2. Professional organizations' trend alerts
 - 3. Summaries of national/regional surveys
- B. Institutional / organizational assessments (general)
 - 1. Type of organization
 - 2. Scope of services

3. Educational relationships
4. Employed / contracted / independent / network relationships
5. Reporting structure / authority / accountability
6. Strategic plan - immediate vs. Long range goals
7. Risk funding structure
8. Mission
9. Prior assessment information

C. Areas for organizational assessment

1. Operational
 - a. Antitrust
 - b. Regulatory/ Licensing
 - c. Business ventures
 - d. Data protection
 - e. Reporting requirements
/mechanisms
 - f. Release of information
 - g. Conflict of interest
 - h. Contract management
 - i. Marketing/media relations
 - j. Complaint management
 - k. External reviews
2. **General liability**
 - a. Facility management
 - b. Plant age
 - c. ownership / lease agreements
 - d. Visitor control procedures
 - e. Accessibility
 - f. Waste management
 - g. Valuables/ inventory control
 - h. Security
 - i. Parking - lighting / location / security
 - j. Safety program
3. **Professional liability**
 - a. Credentialing / reappointment / performance appraisal
 - b. Supervision / monitoring
 - c. Confidentiality
 - d. Products
 - e. Research
 - f. Communication
 - g. Review activities / QI
 - h. Problem reporting systems
 - j. Continuity of care
 - k. Crisis management system
4. **Human resources**
 - a. Workers compensation

- b. Harassment
- c. Negligent hiring / dismissal
- d. Pre-employment testing / evaluation
- e. Drug testing / screening
- f. Grievance procedures

- g. Confidentiality
- h. Education / orientation
- i. Employee health
- j. Employee assistance programs (EAP)

5. New projects and services

- a. "Fit" with existing organizational structure
- b. Identification of insurance needs
- c. Staff requirements
- d. Contract needs
- e. Use of shared services
- f. Competitive impacts
- g. Policy / procedure development
- h. Implementation schedules

6. Construction

- a. Licenses / permits
- b. Contracts
- c. Disruption of existing services
- d. Hazards / environmental impact
- e. Communication
- f. Security
- g. Approvals
- h. Interim Life Safety compliance

IV. KEY COMPONENTS

A. Organizational commitment

- 1. Governing body
- 2. Medical staff
- 3. Administration / management
- 4. Written job responsibilities related to risk program

B. Organizational structure

- 1. Plan approved consistent with organizational objectives
- 2. Designated program coordinator
- 3. Access and accountability
 - a. Senior management
 - b. Medical staff
 - c. Contract staff
 - d. General staff
- 4. Visibility in the organization
- 5. Defined lines of communication and authority

C. Integration with Quality Improvement

- 1. Established relationships
- 2. Operational linkages
- 3. Data sharing
- 4. Confidentiality

D. Physician involvement

1. Input and participation in Risk & Safety Management process
2. Communication and feedback to clinical department
3. Credentialing and reappointment process

- E. Loss prevention and education
 - 1. Defined scope of education
 - a. orientation - general and department specific
 - b. Routine ongoing education ("reorientation")
 - c. Systematic orientation for new / changed situations
 - d. Education as part of performance improvement
 - 2. Program elements
 - a. Consultation
 - b. Assessment and monitoring activities
 - c. Research and analysis
 - d. Responsive to the environment
 - e. Coordination of resources

- F. Contact review
 - 1. Identify role of Risk & Safety Management
 - 2. Define review and signature process
 - 3. Commit to common elements to reduce risk
 - 4. Develop major areas for scrutiny

V. KEY ISSUES IN RISK IDENTIFICATION

- A. Early warning systems
 - 1. Event reports
 - 2. Quality screens
 - 3. Sentinel events
 - 4. Potentially compensable events
 - 5. Claims
 - 6. Product liability issues
 - 7. Follow up calls / visits

- B. Complaints / customer satisfaction
 - 1. Patient / family
 - 2. Medical staff
 - 3. Employees
 - 4. Community / media
 - 5. Complaints

- C. Safety and Security
 - 1. Security reports
 - 2. Committee reports

- D. Medical staff
 - 1. Committee minutes
 - 2. Medical records
 - 3. Credentialing and reappointment
 - 4. Clinical review
 - a. Infection control
 - b. Utilization review

- c. Quality review
- 5. Ethics

- E. Other reviews
 - 1. Safety

2. Licensing and accreditation agencies
3. Internal and external consultants
4. Surveys

VI. RISK ANALYSIS AND TREATMENT

A. Written risk management program

B. Policies and Procedures

1. Release of information
2. Preservation / retention of records / evidence
3. Consent
4. Reuse of disposables
5. Pre-employment process
6. Product selection / recall
7. Patient transfer
8. Credentialing / privileging
9. Contract review
10. Write off/ settlements
11. Patient's rights
12. Orientation and training requirements
13. Access to sensitive areas
14. Problem reporting process

C. Standards of care

1. Internal sources
 - a. Policy and procedure manuals
 - b. Bylaws, rules, regulations of board / medical staff
 - c. Scope of practice / licensure
 - d. Job / position descriptions
 - e. Handouts / notices / memos / directives
2. External sources
 - a. National organizations / societies
 - b. Regulatory and accreditation
 - c. Licensing and certifying agencies
 - d. Consultants / assessment surveyors
 - e. Experts and instructors
 - f. Texts, journals, and other publications

D. Event Investigation

1. Purpose
2. Preservation of evidence
3. Documentation / fact finding
4. Reporting requirements
 - a. Regulatory - state and federal
 - b. Insurance
5. Public relations
6. Communications

E. Claims Administration

1. Definition
2. Loss runs
3. Litigation management
4. Claim file management

- F. Credentialing
 - 1. Pre-application process
 - 2. Delineation of privileges
 - 3. Demonstrated proficiency and competency
 - 4. References
 - 5. orientation
 - 6. Addition / deletion of privileges
 - 7. Insurance coverages
 - 8. Defining privileges across departmental lines
 - 9. Reappointment criteria
 - 10. Allied health professionals
 - 11. Contract employees

- G. Employee related issues
 - 1. Management and supervisory training
 - 2. Breach of contract
 - 3. Wrongful termination
 - 4. Job descriptions
 - 5. orientation and continuing education
 - 6. Employee handbook
 - 7. Policies and procedures
 - 8. Safety
 - a. Universal precautions
 - b. Body mechanics
 - c. Personal safety equipment
 - d. Health screening
 - e. Hazardous communications program
 - f. Security / violence in the workplace
 - g. American's with Disability Act
 - 9. Workers' compensation
 - a. Claims management
 - b. Accident investigation
 - c. Light duty
 - d. Reasonable accommodation
 - e. Rehabilitation
 - f. Analysis for prevention

VII. RISK FINANCING

- A. Definition

- B. Selection criteria
 - 1. Coverage
 - 2. Security
 - 3. Cost

- C. Risk transfer
 - 1. Non insurance
 - a. Transfer of financial obligation/not transfer of legal liability

- b. Stated in contract language
- 2. Insurance

- D. Risk retention
 - 1. Current expense

2. Unfunded reserve
3. Captive
4. Borrowing

VIII. PROGRAM EVALUATION

A. Tangible

1. Loss history
2. Claim "surprises"
3. Third-party evaluations
4. Resource allocation
5. Customer satisfaction surveys
6. Meeting established objectives
 - a. Timely reporting
 - b. Regulatory compliance
 - c. Analyzing events & trends / implementing change
 - d. Support / lead on QI projects

B. Intangible

1. Visibility of program coordinator
2. Accessibility to senior management
3. Impact on policy development
4. Credibility with medical staff
5. Claims that never happen

IX. RISK MANAGEMENT CHALLENGES

- A. Evolving exposures
- B. Health care reform
- C. Medical staff participation
- D. Licensing and regulatory requirements
- E. Third party requirements / requests
- F. Managed care / health networks
- G. Demonstrating value added
- H. Monitoring and evaluation program effectiveness
- I. Creative financing
- J. Mergers and acquisitions
- K. Data management
- L. Continuous quality improvement

M. Confidentiality / release of patient and institutional information


[HOME](#)
[SITE MAP](#)

 SEARCH SITE:

[News, Events & Training](#)
[Design Guidance](#)
[Project Management](#)
[Mandates / References](#)

Design Guidance

[Building Types](#)
[Design Objectives](#)
[Products & Systems](#)

■ ■ Threat/Vulnerability Assessments & Risk Analysis

by Nancy A. Renfroe and Joseph L. Smith
 Applied Research Associates, Inc.

[View resource pages linked to this topic](#)



[Printable vers](#)

Introduction

All facilities face a certain level of risk associated with various threats. These threats can be the result of natural events, accidents, or intentional acts to cause damage. Depending on the nature of the threat, facility owners have a responsibility to limit exposure to these threats to the extent possible. The federal government has established the Interagency Security Committee (ISC) Security Criteria. The ISC Security Criteria states,

"The application of the Security Design Criteria is based on a project-specific risk assessment that looks at threat, vulnerability, and consequences, components of risk . . . The building's specific security requirements are based on a risk assessment - done at the earliest stages of programming."

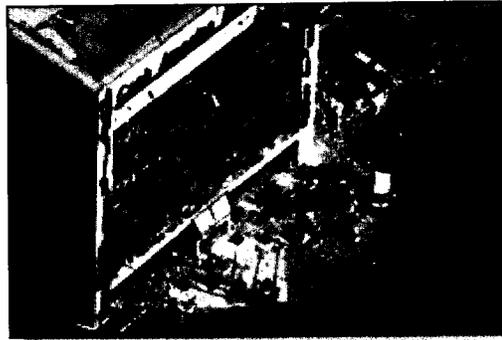
Facility owners, particularly owners of public facilities, should adhere to the ISC Security Design Criteria as those put forth in the ISC Security Design Criteria. The desire to lease space to federal government agencies must implement the ISC Security Design Criteria in the design of new facilities and/or the renovation of existing facilities.

Description

A. Threat Assessment

The first step in a risk management program is a threat assessment. A threat assessment considers the full spectrum of threats (i.e., natural, criminal, accidental, etc.) for a given facility/location. The assessment should consider historical information to evaluate the relative likelihood of occurrence for each threat. Historical data concerning frequency of occurrence for given threats, such as tornadoes, hurricanes, floods, fire, or earthquakes can be used to evaluate the credibility of the given threat. For criminal threats, the crime rates in the area can provide a good indicator of the type of criminal activity that may threaten the facility. In addition, the type of assets and/or activity located in the facility may target attractiveness in the eyes of the aggressor. The type of asset located in the facility will also relate directly to the likelihood of various types of accidents. For example, a facility that utilizes heavy industrial machinery has a higher risk for serious or life-threatening job related accidents than a typical office building.

Figure 1. The torn and damaged Cash An Building—Fort Worth, Texas. (Courtesy of kenku)



For terrorist threats, the attractiveness of the facility as a target is a consideration. In addition, the type of terrorist act may vary based on adversary and the method of attack most likely to be successful. For example, a terrorist wishing to strike against the federal government to attack a large federal building than to attack a multi-tenant office building. A large number of commercial tenants and a few government tenants at the large federal building makes mounting a successful attack too difficult. An attack may be diverted to a nearby facility that may not be as attractive from a security perspective, but has a higher probability of success due to the absence of security. In general, the likelihood of terrorist attacks cannot be quantified since terrorism is, by its very nature random. Hence, when considering the concept of developing credible threat packages is important.

B. Vulnerability Assessment

Once the credible threats are identified, a vulnerability assessment is conducted. The vulnerability assessment considers the potential impact of loss of the facility as well as the vulnerability of the facility/location to an attack. The degree to which the mission of the agency is impaired by a successful attack given threat. A key component of the vulnerability assessment is providing ratings for impact of loss and vulnerability. These definitions may vary from facility to facility. For example, the amount of time that mission capabilities are lost is an important part of impact of loss. If the facility being assessed is a Control Tower, a downtime of a few minutes may be a serious impact. For a Social Security office a downtime of a few minutes would be minor. The definitions for impact of loss is provided below. These definitions are for facilities that generates revenue by serving the public.

- **Devastating:** The facility is damaged/contaminated beyond repair. Items/assets are lost, destroyed, or damaged beyond repair/replacement. The number of visitors to other facilities in the organization may be reduced by 75% for a limited period of time.
- **Severe:** The facility is partially damaged/contaminated. Example: a structure breach resulting in weather/water, smoke, impact, or contamination of areas. Some items/assets in the facility are damaged beyond repair/replacement. The entire facility may be closed for a period of several weeks and a portion of the facility may be closed for an extended period (more than one month). Some assets may need to be moved to protect them from environmental damage. The number of visitors to other facilities in the organization may be reduced by up to 50% for a limited period of time.

time.

- **Noticeable:** The facility is temporarily closed or unable to operate without an interruption of more than one day. A limited amount of equipment may be damaged, but the majority of the facility is not affected. Visitors to this and other facilities in the organization may be restricted for a limited period of time.
- **Minor:** The facility experiences no significant impact on operations (less than four hours) and there is no loss of major assets.

Vulnerability is defined to be a combination of the attractiveness of the target and the level of deterrence and/or defense provided by the existing countermeasures. Target attractiveness is a measure of the asset or facility in the eyes of a potential adversary and is influenced by the function and/or symbolic importance of the facility. The definitions for vulnerability ratings are as follows:

- **Very High:** This is a high profile facility that provides a very attractive target and the level of deterrence and/or defense provided by the existing countermeasures is inadequate.
- **High:** This is a high profile regional facility or a moderate profile facility that provides an attractive target and/or the level of deterrence and/or defense provided by the existing countermeasures is inadequate.
- **Moderate:** This is a moderate profile facility (not well known nationally or regionally) that provides a potential target and/or the level of deterrence and/or defense provided by the existing countermeasures is marginal.
- **Low:** This is not a high profile facility and provides a possible level of deterrence and/or defense provided by the existing countermeasures that is adequate.

The vulnerability assessment may also include detailed analysis of the potential damage and loss from an explosive, chemical or biological attack. Professional engineering training and experience in these areas are required to perform these analyses. A sample of the type of output that can be generated by a detailed vulnerability assessment is shown in Figure 2. This graphic representation of the potential damage from an explosive attack allows a building owner to quickly interpret the results of the analysis, although a more fully detailed and quantitative engineering response is required to design a retrofit upgrade. In addition, similar representations can be used to show the response of an upgraded facility to the same explosive threat. This allows the building owner to interpret the potential benefit that can be achieved by implementing structural upgrades to the building frame, wall, roof and/or windows.

Red = High Hazard
 Yellow = Medium Hazard
 Green = Low Hazard
 Blue = Unbroken

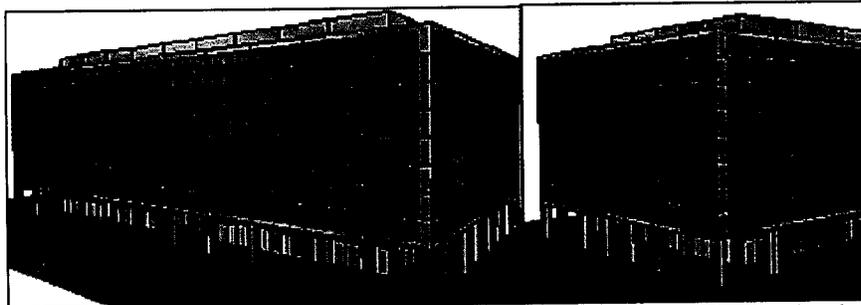


Figure 2. Sample output from detailed explosive analysis: glazing hazard facility (left) and glazing hazard in upgraded facility (right)

C. Risk Analysis

A combination of the impact of loss rating and the vulnerability rating evaluate the potential risk to the facility from a given threat. A sample is depicted in Table 1. High risks are designated by the red cells, moderate risks by the yellow cells, and low risks by the green cells.

Table 1. Matrix identifying levels of risk

	Vulnerability to Threat		
Impact of Loss	Very High	High	Moderate
Devastating			
Severe			
Noticable			
Minor			

The ratings in the matrix can be interpreted using the explanation shown in Table 2.

Table 2. Interpretation of the risk ratings

High	These risks are high. Countermeasures recommended to mitigate these risks should be implemented as soon as possible.
Moderate	These risks are moderate. Countermeasure implementation should be planned in the near future.
Low	These risks are low. Countermeasure implementation to enhance security, but is of less urgency than the other risks.

D. Upgrade Recommendations

Based on the findings from the risk analysis, the next step in the process is to recommend upgrades to the facility.

countermeasure upgrades that will lower the various levels of risk. If countermeasures for a given facility level are not currently present, countermeasures should automatically be included in the upgrade recommendation. Additional countermeasure upgrades above the recommended minimum should be recommended as necessary to address the specific threat to the facility. The estimated capital cost of implementing the recommended countermeasures is usually provided. The estimated installation and operating costs for countermeasures are also usually provided. All operating costs are estimated on a per year basis.

E. Re-Evaluation of Risks

The implementation of the recommended security and/or structural countermeasures have a positive effect on the impact of loss and/or the vulnerability rating of the threat. The final step in the process is to re-evaluate these two ratings in light of the recommended upgrades. Using an exterior explosive threat as an example, the installation of window retrofits (i.e., security window film, laminated glass) will not prevent the explosive attack from occurring, but it should reduce the impact of loss/injury caused by hazardous flying glass. Therefore, the impact of the explosive threat would improve, but the vulnerability rating would stay the same.

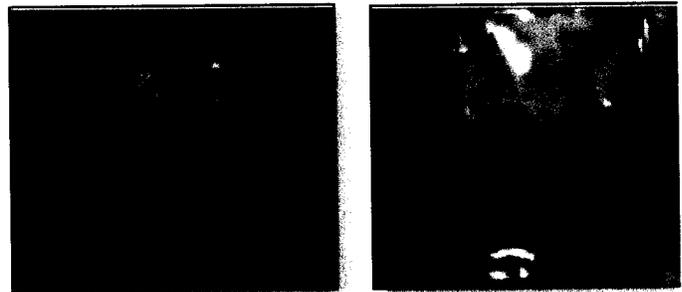


Figure 3. The above photos depict two windows subjected to a large exterior explosive threat. The unprotected window on the left fails catastrophically. The protected window on the right retains glass fragments and poses a significantly lower hazard.

F. Summary

The overall threat/vulnerability and risk analysis methodology is summarized in the following flowchart.

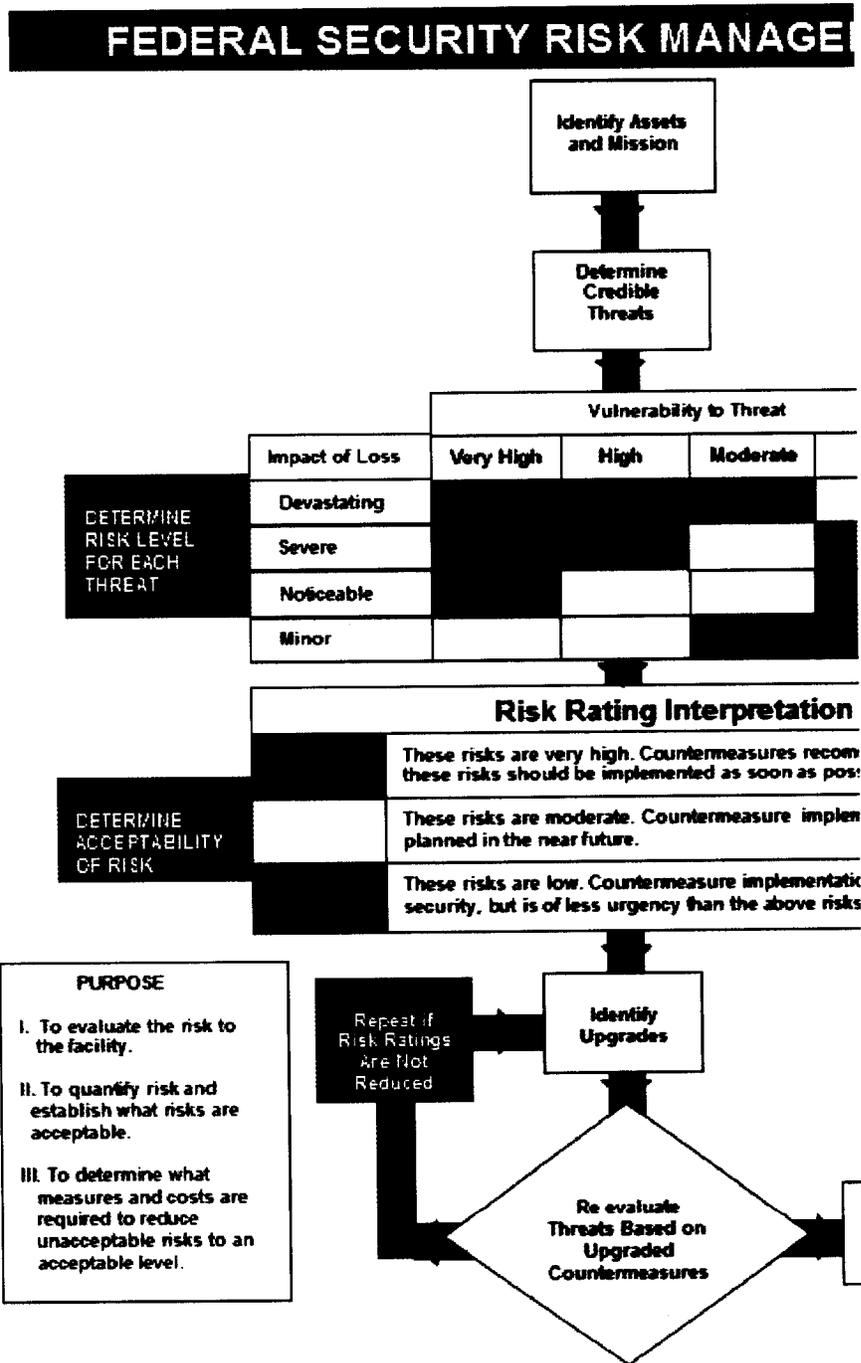


Figure 4. Flowchart depicting the basic risk assessment pro

Application

Threat/vulnerability assessments and risk analysis can be applied to an organization. The federal government has been utilizing varying types of threat/vulnerability assessments and analyses for many years. Currently, the General Services Administration is utilizing a methodology entitled Federal Security Risk Management. This process is basically the process described in this Resource Page. The General Services Administration process to assess over 8000 federally owned and/or leased facilities. The Internal Revenue Service (IRS) has also adapted this same methodology to

facilities housing IRS employees. Other agencies that have used th some of their facilities include the U.S. Department of Agriculture ar Institution. The Social Security Administration has also trained over managers and security specialists to apply this process.

Relevant Codes & Standards

Executive Order 12977, "Interagency Security Committee"
Interagency Security Committee (ISC) Security Design Criteria - De
classifications and resultant federal protective design requirement
Unified Facilities Criteria (UFC) - *UFC 4-010-01 DoD Minimum Anti*
for Buildings - Establishes prescriptive procedures for Threat, Vuli
assessments and security design criteria for DoD facilities (Officia
Federal Emergency Management Agency (FEMA) - *Publication No.*
Human-Caused Hazards into Mitigation Planning

Additional Resources

WBDG:

Safe - Ensure Occupant Safety & Health; Safe - Plan for Fire Prot
Security of Assets; Safe - Resist Natural Hazards

Federal Agencies:

Blast Mitigation Action Group - US Army Corps of Engineers grou
Threat, Vulnerability and Risk Assessments of USACE operatec
facilities.

All-Hazard Mitigation Program on Anti-terrorism - Federal Emerger
Agency (FEMA)

Office of Federal Protective Service (FPS) - Security organization
and Vulnerability and Risk Assessments and operational securit
managed by GSA.

Design & Analysis Tools:

FSR-Manager - Proprietary software developed by Applied Resea
to assist in performing threat/vulnerability assessments and risk
RAMPART™ (Assessment Method - Property Analysis and Ranki
by Sandia National Laboratories and NeoSafety as a screening-
program to determine the risk to a building by natural hazards, c

Organizations & Associations:

American Society of Industrial Security (ASIS) - A leading non-pro
security managers, product manufacturers and consultants offer
publications and programs including Threat and Vulnerability As
International Association of Professional Security Consultants - Ai
security consultants whose members frequently perform Vulner

Publications:

Are Your Tenants Safe? by Building Owners and Managers Assoc
template and instructions for completing a Threat, Vulnerability &

on commercial and institutional properties. Availability: BOMA
*Multihazard Identification and Risk Assessment: A Cornerstone of
Mitigation Strategy* by Federal Emergency Management Agency
Washington, DC: U.S. Government Printing Office, 1997. Availa

Updated: 11-18-2002



Disclaimer • If you have suggestions or want to comment on this website, please contact us:

National Institute of Building Sciences (NIBS)
1090 Vermont Avenue NW, Suite 700 • Washington, DC 20005
202.289-7800 • Fax 202.289.1092 • info-wbdg@nibs.org