NIST Special Publication 500-174

Guide for Selecting Automated Risk Analysis Tools

Irene E. Gilbert

Technology

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology

The National Institute of Standards and Technology[1] was established by an act of Congress on March 3, 1901. The Institute's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Institute conducts research to assure international competitiveness and leadership of U.S. industry, science and technology. NIST work involves development and transfer of measurements, standards and related science and technology, in support of continually improving U.S. productivity, product quality and reliability, innovation and underlying science and engineering. The Institute's technical work is performed by the National Measurement Laboratory, the National Engineering Laboratory, the National Computer Systems Laboratory, and the Institute for Materials Science and Engineering.

The National Measurement Laboratory

Provides the national system of physical and chemical measurement; coordinates the system with measurement systems of other nations and furnishes essential services leading to accurate and uniform physical and chemical measurement throughout the Nation's scientific community, industry, and commerce; provides advisory and research services to other Government agencies; conducts physical and chemical research; develops, produces, and distributes Standard Reference Materials; provides calibration services; and manages the National Standard Reference Data System. The Laboratory consists of the following centers:

- Basic Standards[2]
- Radiation Research
- Chemical Physics
- Analytical Chemistry

The National Engineering Laboratory

Provides technology and technical services to the public and private sectors to address national needs and to solve national problems; conducts research in engineering and applied science in support of these efforts; builds and maintains competence in the necessary disciplines required to carry out this research and technical service; develops engineering data and measurement capabilities; provides engineering measurement traceability services; develops test methods and proposes engineering standards and code changes; develops and proposes new engineering practices; and develops and improves mechanisms to transfer results of its research to the ultimate user. The Laboratory consists of the following centers:

- Computing and Applied Mathematics
- Electronics and Electrical Engineering[2]
- Manufacturing Engineering
- Building Technology
- Fire Research
- Chemical Engineering[3]

The National Computer Systems Laboratory

Conducts research and provides scientific and technical services to aid Federal agencies in the selection, acquisition, application, and use of computer technology to improve effectiveness and economy in Government operations in accordance with Public Law 89-306 (40 U.S.C. 759), relevant Executive Orders, and other directives; carries out this mission by managing the Federal Information Processing Standards Program, developing Federal ADP standards guidelines, and managing Federal participation in ADP voluntary standardization activities; provides scientific and technological advisory services and assistance to Federal agencies; and provides the technical foundation for computer-related policies of the Federal Government. The Laboratory consists of the following divisions:

- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

The Institute for Materials Science and Engineering

Conducts research and provides measurements, data, standards, reference materials, quantitative understanding and other technical information fundamental to the processing, structure, properties and performance of materials; addresses the scientific basis for new advanced materials technologies; plans research around cross-cutting scientific themes such as nondestructive evaluation and phase diagram development; oversees Institute-wide technical programs in nuclear reactor radiation research and nondestructive evaluation; and broadly disseminates generic technical information resulting from its programs. The Institute consists of the following divisions:

- Ceramics
- Fracture and Deformation[3]
- Polymers
- Metallurgy
- Reactor Radiation

[1]Headquarters and Laboratories at Gaithersburg, MD, unless otherwise noted; mailing address Gaithersburg, MD 20899.
[2]Some divisions within the center are located at Boulder, CO 80303.
[3] Located at Boulder, CO, with some elements at Gaithersburg, MD.

NIST Special Publication 500-174

Guide for Selecting Automated Risk Analysis Tools

Irene E. Gilbert

Computer Security Division
National Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

October 1989

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Raymond G. Kammer, Acting Director

NIST

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) (formerly the National Bureau of Standards) has a unique responsibility for computer systems technology within the Federal government. NIST's National Computer Systems Laboratory (NCSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. NCSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. NCSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 500 series reports NCSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

Library of Congress Catalog Card Number: 89-600769
National Institute of Standards and Technology Special Publication 500-174
Natl. Inst. Stand. Technol. Spec. Publ. 500-174, 34 pages (Oct. 1989)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1989

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

EXECUTIVE SUMMARY

This document recommends a process for selecting automated risk analysis tools. It is primarily intended for managers and those responsible for managing risks in computer and telecommunications systems. The document describes important considerations for developing selection criteria for acquiring risk analysis software. The information presented is derived from reviews of risk analysis software tools in the Risk Management Research Laboratory which is cooperatively sponsored by the National Institute of Standards and Technology (NIST) and the National Computer Security Center (NCSC) and from experiences of organizations in the Federal government and private sectors.

This document recommends selecting a group of personnel with special skills to participate in the risk analysis studies. Concepts and definitions of terms necessary to understand risk analysis are also provided This report describes three essential elements that should be present in an automated risk analysis tool: data collection, analysis, and output results.

When developing site-specific requirements criteria, mandatory requirements should be separated from those that are desirable. The evaluation weighting factors for desirable requirements can be separated into high, medium, and low priority items. Appendix A contains a questionnaire and a selection checklist.

To assist in defining requirements that will permit logical evaluation of risk analysis tools, this report makes the following recommendations:

- An automated risk analysis tool should contain modules for data collection, analysis, and output results (Section 3.1).

- The automated risk analysis tool selected should be compatible with the hardware and software in use at the organization. Hardware and software processing requirements must be defined for each computer system, application, or facility being reviewed (Section 3.2.1).

- The risk analysis methodology should reflect the organization's policy on using risk analysis tools and should be explicitly stated in the requirements definition (Section 3.2.2).

- Effective reporting of the risk analysis results will help managers to weigh the alternatives and to select reliable and cost-effective safeguards. Therefore, the types of information expected in the output reports should be clearly defined (Section 3.2.3).

- Documentation describing the tool in over-all terms is essential to its effective use. It is important to establish criteria for evaluating the quality of documentation supplied with the tool (Section 3.2.4).

- The ability to maintain a history of the information collected during the data collection phase of the analysis is useful in subsequent reviews or queries (Section 3.2.5).

- Automated risk analysis tools generally are efficient and error-free although some incur excessive overhead in the installation and efficient use of the product. The best precaution against this risk is to obtain vendor installation and training support. Evaluations from current users will be of value (Section 3.2.6).

- Effective use of any risk analysis tool depends, in part, on how well the analyst is trained. Guidance on installation and use of the product is essential. The intentions of the product developer regarding installation, training, and ongoing product support should be explicitly stated in writing before purchasing the tool. Each of these issues may be negotiable (Section 3.2.7).

- Understanding fees charged by each competing vendor is an important part of any software purchase. Costs to be evaluated include installation fees, training, and ongoing software support and maintenance. Additional costs may be incurred for site-specific modifications and multiple-site purchases (Section 3.2.8).

GUIDE FOR SELECTING AUTOMATED RISK ANALYSIS TOOLS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. INTRODUCTION 1

1.1 Background and Historical Perspectives 1

1.2 Purpose and Scope 1

1.3 Document Overview 1

2. CONCEPTS AND TERMS 2

2.1 Risk Management 2

2.1.1 Safeguard Selection 2

2.1.2 Certification and Accreditation 3

2.1.3 Contingency Planning 3

2.2 Risk Analysis 3

2.2.1 Benefits of Performing a Risk Analysis 4

2.2.2 When to Use Risk Analysis 4

2.2.3 Participants in the Risk Analysis 4

2.3 Considerations for Selecting Commercially Available Tools 5

2.4 Advantages and Disadvantages of Currently Available Tools 6

2.5 Additional Concepts and Terms 6

2.6 Summary 9

3. SELECTING AUTOMATED RISK ANALYSIS TOOLS 10

3.1 Fundamental Elements of A Risk Analysis Tool 10

3.1.1 Data Collection 10

3.1.2 Analysis 12

3.1.3 Output Results 13

3.2 Site-Specific Selection Criteria 14

3.2.1 Hardware and Software Compatibility 14

3.2.2 Methodology 15

3.2.3 Reporting Requirements 15

3.2.4 Documentation 16

3.2.5 History and Security Features 16

3.2.6 Utility and Ease of Use 16

3.2.7 Training and Technical Support 17

3.2.8 Cost 17

3.3 Summary 18

Appendices

A. The Selection Process 19

B. References 24

1. INTRODUCTION

Murphy's Law makes the observation that "anything that can go wrong, will go wrong," but, not necessarily with the probability of one. Managers of computer systems should be aware of this point in managing risks. For example, there is the threat of nuclear attack, but how many of us have invested in a bomb shelter? We can conclude that the investment is too high and the probability too low, even though the result of the threat occurrence would be disastrous. In this regard, managers of computer systems must not ignore the answers to such questions as: What can go wrong, and how likely is it to happen? What are the consequences of the occurrence of certain threats, and how can they be mitigated? How much risk can be tolerated, and how can these risks be quantified and managed?

1.1 Background and Historical Perspectives

Every Federal agency is required to conduct periodic risk analysis of its computer systems. In the 1970's, the Federal government attempted to formalize the risk analysis process. This process prescribed a methodology for performing risk analysis in large data processing centers. Today, this methodology is not suitable for applications, networks, or small systems environments so prevalent in many organizations. Over the years, risk analysis technology has continued to evolve, creating a quandary for those who seek to select the best risk analysis tools for their needs.

1.2 Purpose and Scope

This guide is intended to assist managers in selecting the most appropriate risk analysis tool. The scope of the document is narrow and is not intended as a tutorial on risk analysis. Rather, considering the diversity of tools in the market place, this document contains guidance on developing evaluation and selection criteria.

1.3 Document Overview

The document is divided into three sections. Section 1 provides describes the purpose and scope of the guide. Section 2 introduces the reader to basic risk management concepts and terms. The benefits of risk analysis are discussed along with the advantages and disadvantages of automated tools currently in use. Section 3, provides guidance in developing requirements for hardware and software, methodology, reports generation, documentation, security controls, training and support, and cost. For each category of criteria discussed, a description is presented of risk analysis tools currently available.

Appendix A contains a list of questions and a checklist to aid in the evaluation process. References are provided in Appendix B for those who seek additional information on recent work in risk analysis techniques.

2. CONCEPTS AND TERMS

This section presents basic concepts and terms used by risk analysis and management software tools. The relationship between risk analysis and risk management is briefly reviewed because they are closely correlated. This section also explains the advantages and disadvantages of risk analysis tools currently in use. However, no attempt is made to describe the capabilities of specific tools. This information is available upon request[1] [DESC89].

2.1 Risk Management

Risk management encompasses the entire spectrum of activities (including physical, technical, and administrative controls and procedures) that leads to cost-effective security solutions. Risk management seeks to achieve the most effective safeguards against accidental and deliberate attacks against a computer system. A risk management program has three fundamental elements: safeguard selection, certification and accreditation, and contingency planning.

Managing risks means not only identifying threats but also determining their impact and severity. Some threats require extensive controls while others require few. Certain threats, such as viruses and other computer crimes, have been highlighted through extensive press coverage causing too many safeguards to be implemented in some cases. On the other hand, repeated errors by employees may receive only minor consideration. Yet, statistics reveal that errors and omissions generally cause more harm than virus attacks. Resources are often expended on threats not worth controlling, while other major threats receive little or no control. Until managers understand the magnitude of the problem and the areas in which threats are most likely to occur, protecting vital computer resources will continue to be an arbitrary and ineffective proposition.

2.1.1 Safeguard Selection

Safeguard selection is an important function of risk management and may also be an integral component of some risk analysis tools. Whether or not a safeguard selection step is included in the risk analysis tool, managers still have responsibility to select safeguards that will mitigate certain threats. The likelihood of the occurrence of threats normally cannot be reduced to zero in a cost-effective manner. Therefore, managers should determine a tolerable level of risk and implement cost-effective safeguards that will reduce losses to an acceptable level. Safeguards may act in several ways:

---

[1]Description of commercial products does not imply the endorsement or approval of NIST or the U.S. Government.

- o reduce the likelihood of the occurrence of threats
- o reduce the impact of threat occurrences
- o facilitate recovery from threat occurrences

When selecting safeguards, management should focus on areas with the greatest potential for loss or harm. Safeguards must be cost-effective returning more in savings than initial costs.

2.1.2 Certification and Accreditation

Certification and accreditation are important elements of managing risks in computer environments. Certification is the technical verification that the safeguards and controls selected for an application or computer system are adequate and function properly [FIPS102]. Accreditation is official authorization for operation, security corrections, or suspension of certain activities.

2.1.3 Contingency Planning

Contingency planning ensures a continued processing capability for critical systems in the event of an unexpected computer outage [FIPS87, SP500-85, SP500-134].

2.2 Risk Analysis

Risk analysis is the cornerstone of risk management. It is a procedure used to estimate potential losses that may result from system vulnerabilities and the damage from the occurrence of certain threats. Risk analysis identifies not only critical assets that must be protected but considers the environment in which these assets are stored and processed. The ultimate purpose of risk analysis is to help in the selection of cost-effective safeguards that will reduce risks to an acceptable level.

Most methods of risk analysis initially require the identification and valuation of assets. From this point on, they proceed differently in developing loss computations. Most risk analysis tools, however, can be categorized as either quantitative or qualitative. That is, some produce results expressed in monetary or economic terms (quantitative), while others make use of qualitative expressions or approximations. Based on the outcome of the analysis, a series of control measures or safeguards may be selected which are both cost-effective and which provide the necessary level of protection.

2.2.1 Benefits of Performing a Risk Analysis

Risk analysis forms the basis for establishing a cost-effective risk management program. Risk management ensures that reasonable steps have been taken to prevent situations which can interfere with accomplishing the organization's mission.

This next point may seem obvious, but it is not uncommon for a manager to select a safeguard without first doing a risk analysis. The result may be a serious over-expenditure of funds for protective measures. Even worse, the implemented safeguards may not adequately reduce the actual (undefined) risks. A prudent manager will factor their judgment into a risk analysis [FIPS31].

2.2.2 When to Use Risk Analysis

Risk analysis is most useful when applied during the system design phase of an application or system so that potential losses may be identified and security requirements defined right from the start. Experience has shown that implementing security controls during the design phase is far less costly than retrofitting such controls after a computer system is operational. Nonetheless, for those systems already in operation, risk analysis can identify vulnerabilities for which corrective action can be taken. Risk analysis conducted during any phase of a computer system life cycle should use an approach for reducing the loss of personnel efficacy, information, equipment, and processing capability.

2.2.3 Participants in the Risk Analysis

Generally, performance of risk analysis increases staff awareness of potential problems and strengthens the risk management program. In the past, the responsibility of managing risks was that of the Automatic Data Processing (ADP) Manager. This approach has changed, and now many groups within an organization share the responsibility for a successful risk management program and for conducting a risk analysis. A risk analysis team composed of the following members is recommended:

1. The risk analyst (the individual assigned to conduct the risk analysis) is responsible for gathering the input data. The analyst has further responsibility for presenting the best possible information for safeguard selection to senior management.

2. Users are responsible for providing accurate information about their applications to the risk analyst. Other support functions such as Building Engineering, Personnel, Physical Security, and others can provide information about environmental and outside threats.

3. The ADP Operations staff is responsible for supplying information about hardware, software, and procedural functions.

4. Senior Management is responsible for ensuring the protection of organizational assets. Specifically, senior management should do the following:

- o Demonstrate to all levels of the organization a firm commitment to planning and supporting a risk management program. This can be accomplished through issuance of a policy statement.

- o Assign responsibility to manage the risk management program.

- o Commit the resources necessary to conduct risk analysis and carry out the risk management program.

- o Require periodic monitoring of safeguards and controls to ensure their continued adequacy.

2.3 Considerations for Selecting Commercially Available Tools

There are obvious advantages in selecting commercially available risk management tools over in-house developed systems. The first is immediate availability. The second is the ability to evaluate the quality of the software before money is committed. Unlike an automated risk analysis tool developed in-house, the supplier usually has programming expertise and awareness of the complex logic often necessary in this kind of application. The supplier also typically provides a maintenance agreement which relieves the organization of maintaining the software. Additionally, the cost to develop a risk analysis tool in-house may be higher than the purchase of commercially available software. Thus, the primary advantages of acquiring commercially available risk analysis software are:

- o Immediate availability
- o Known quality
- o Specialized knowledge
- o No in-house maintenance
- o Lower cost

When the organization has unique requirements that are not met by the current capabilities of a tool, consider requesting that the developer modify the tool. If the developer is unwilling or unable to do so, consider another tool. Many developers, however, are willing to make needed modifications.

2.4 Advantages and Disadvantages of Currently Available Tools

Clearly there are benefits and limitations to any automated risk analysis methodology. Site-specific criteria must be established before a preferred methodology can be selected. Some advantages and disadvantages of current automated risk analysis tools follow.

Advantages

Unlike manual risk analysis that usually take months to complete, the automated methodology can evaluate system weaknesses in a much shorter time frame. The analysis can be carried out quickly enough to ensure that the results are not outdated by changes in the system.

Further, automated risk analysis tools are easily adaptable to operational and administrative systems of all sizes, and generally allow the user to quickly explore the results of implementing certain safeguards. Some tools are suitable for use during system development as well as for the analysis of operational systems.

Disadvantages

A major disadvantage is that there is no standard method or agreed upon approach for performing risk analysis, and there is no assurance that any particular method is complete or accurate. This can make it difficult for users to select the best risk analysis tool for their needs. The root questions in analyzing these tools must be, "What is the tool measuring, and are the results useful?"

2.5 Additional Concepts and Terms

Assets

Identifying system assets is the central feature of the risk analysis process. The risk analysis methodology should allow the risk analyst to define exactly what is to be protected and its value. In the past, risk analysis concentrated on the physical hardware components. Today, software, data, and documentation are the primary focus.

Assets may be categorized as tangible and intangible and include the following:

Tangible	Intangible
o Facilities	Personnel
o Hardware	Reputation
o Software	Motivation
o Supplies	Morale
o Documentation	Goodwill
o Data	Opportunity

Annual Loss Exposure (ALE)

Annual loss exposure is the projected loss (in dollars) that one can expect to lose with a computer system in a year.

Likelihood of Occurrence

The likelihood of occurrence is a measure of the probability of a loss-causing event.

Risk

The degree of loss.

State

A description of the system under analysis and its environment at a given moment.

Sensitive Information

Sensitive information means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. [2]

---

[2]Computer Security Act of 1987 (P.L. 100-235).

Safeguards

Safeguards are physical controls, mechanisms, policies and procedures that protect assets from threats. Examples of safeguards are fences, alarms, guards, sprinklers, passwords, access controls, policy statements, offsite storage, tempest shielding, and so forth. In order for a threat to occur, one or more of the safeguards must be bypassed or circumvented entirely or in part.

The kinds of safeguards selected will depend upon the intended function of the assets and their value. In civilian government agencies, availability and integrity of assets may be of primary concern, while confidentiality may play a greater role in the military community.

Safeguards System

A safeguards system is the complete collection of all safeguards. The ability to identify countermeasures or safeguards systems that will reduce vulnerabilities and thereby the risks is an essential component of managing risks.

Safeguard Cost/Benefit Analysis

Security expenditures should be cost-justified just like every other expenditure. Thus, the key to the selection of optimum security measures is the ability to estimate the reduction in loss after the implementation of certain safeguards. A safeguard cost/benefit analysis enables the manager to easily develop justification for the acquisition of each safeguard. The cost of security measures should compare favorably with the reduction of expected future losses.

Threat

A threat is a person, thing, event, or idea which poses some danger to an asset. The occurrence of a threat may compromise the confidentiality, integrity, or availability of an asset by exploiting vulnerabilities or weaknesses in the system. Threats may fall into two categories: unintentional (accidental) or intentional (deliberate.

Unintentional acts include events and occurrences such as:

Errors caused by people	Equipment failures
Natural disasters	Communications malfunctions

Intentional acts include incidents such as:

Theft	Vandalism
Sabotage	Misuse of resources

There are many more common occurrences of threats which include the following:

- o eavesdropping/wire tapping
- o disclosure of proprietary information
- o unauthorized use of hardware and software
- o violation of software licensing agreements
- o power interruptions
- o environmental failures and accidents
- o static electricity discharge
- o terrorist acts

Threat Agent

An entity that might initiate a threat occurrence.

Vulnerabilities

Vulnerabilities are weaknesses in the safeguard's system, or the absence of a safeguard. No matter which definition is used, vulnerabilities can clearly be associated with threats: the threat of fire is associated with the vulnerability of having inadequate fire protection; the threat of unauthorized access can be linked to the inadequacy of access controls; and the threat of losing critical data and processing support lies in ineffective contingency planning.

Consequence

A consequence (sometimes referred to as outcome) refers to the undesirable result of a threat's action against the asset which results in measurable loss to the organization.

2.6 Summary

This section has introduced the concept of managing risks and has shown why it is important. It has described the relationship between risk management and risk analysis. The principal participants required to conduct a risk analysis have been identified along with the shortcomings of using currently available tools. Several important terms have been introduced, including: assets, threats, vulnerabilities, consequences, likelihood of occurrence, and safeguards. These are all issues with which risk analysis deals.

3. SELECTING AUTOMATED RISK ANALYSIS TOOLS

There are many risk analysis techniques being used today, all of which have value. Selecting the most appropriate tool requires planning and preparation. This section presents an overview of risk analysis tools currently in use and provides an approach for their selection.

3.1 Fundamental Elements of A Risk Analysis Tool

A comprehensive risk analysis tool consists of three fundamental steps:

- o Data collection
- o Analysis
- o Output results

Not only should the risk analysis tool meet this basic criteria, it should meet organizational requirements as well. A discussion on developing site-specific requirements follows in section 3.2.

3.1.1 Data Collection

First, an automated risk analysis tool should have a structure for gathering information either textually or graphically about the system under study. This phase is necessary to derive a description of the assets and their value to the organization. It should be possible to gather information about threat events, vulnerabilities, and safeguards as well. An asset will be defined in terms of its value to the organization, a threat event in terms of its undesirability, a vulnerability in terms of system weaknesses, and a safeguard in terms of its effectiveness.

Asset Identification and Valuation

The asset identification phase is generally accepted as the most important step in the risk analysis process for it provides management an awareness of the need for security, or it may point out that there is nothing of substantial value in the application under review that needs protecting. Many risk analysis tools evaluate tangible assets, such as facilities and material, and intangible assets, such as organizational reputation and employee motivation and morale. Many consider the cost of replacing software, data, and documentation as well as physical and environmental controls.

Assets may include but are not limited to the following categories:

- o Information
- o Equipment
- o Inventories
- o Personnel
- o Services
- o Real estate
- o Income

Threat Assessment

The next component to be identified in the data collection phase is the identification of threats that have the potential to compromise the security of an asset. Unlike assets, which differ from one organization to another, threats are more generic. A taxonomy of threats such as those of Carroll [Carr84] and Parker [PARK81] is useful to identify potential threats. There are other sources of information on threats as well. For example, many organizations collect statistics on the occurrence rate of certain events (i.e., system malfunctions, operator errors, etc.). Law enforcement agencies maintain databases on computer crimes. The National Oceanographic and Atmospheric Administration (NOAA) provides information on natural hazards. All available sources should be used to determine conceivable threats and their likelihood of occurrence.

Vulnerability Assessment

Understanding vulnerabilities that can contribute to the occurrence of threat events is an important aspect of identifying losses. Some risk analysis tools treat vulnerabilities as weaknesses in the safeguards systems that allow threats to compromise the confidentiality, integrity, or availability of an asset. Others treat vulnerabilities as the absence of safeguards or controls that would prevent security violations. No matter which approach is taken by a risk analysis tool, security risks cannot be determined without knowledge of how vulnerable the system is to potential threats.

Safeguards Effectiveness

The next element that should be addressed by the risk analysis tool is the relative effectiveness of controls and safeguards currently in place. The numerous safeguards to be evaluated, may be categorized as follows:

- o Administrative security
- o Physical facilities security
- o Software security
- o Hardware security

- o Personnel security
- o Environmental security
- o Communications security

It should be possible for the automated tool to gather information in each of these categories for use in the analysis.

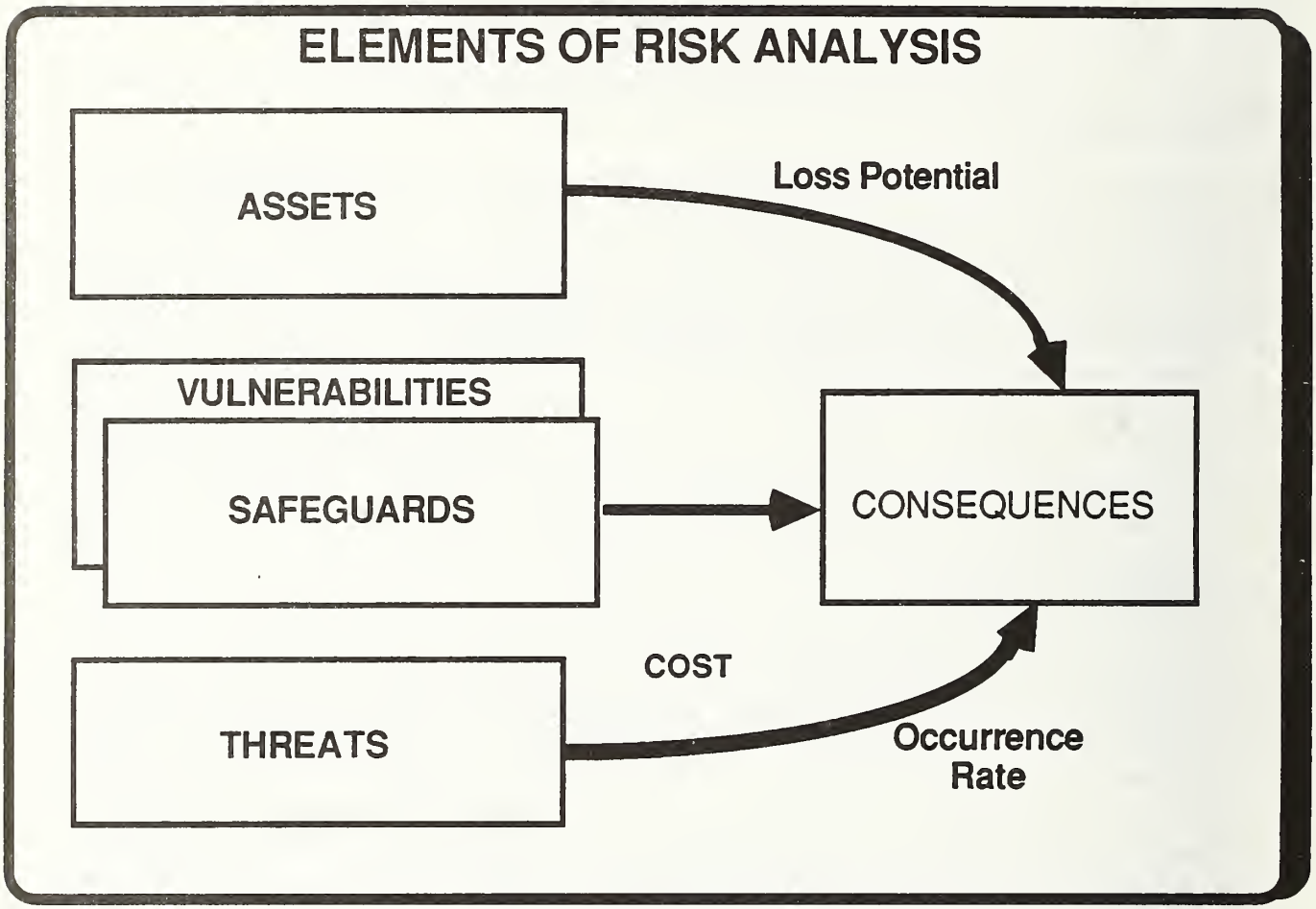

FIGURE 1

3.1.2 Analysis

The analytical process (methodology) analyzes the relationships between assets, threats, vulnerabilities and/or safeguards, and possibly other elements (i.e., likelihood of occurrence) to determine potential losses. Current techniques for measuring loss include orders of magnitude estimates, fuzzy reasoning, event trees, fault trees, and others. Some automated risk analysis tools use the traditional quantitative approach for calculating risks

as described in FIPS Publication 65. Using this approach an approximation of loss (i.e., Annual Loss Expectancy (ALE)) is obtained by estimating for each data file or application system the frequency of occurrence of events that affect data integrity, confidentiality, or processing capability and the impact (in dollars) that could result. FIPS 65 recognized that exact impact and frequency could not usually be specified and suggested an "orders of magnitude approach" for estimating the consequences of undesirable events.

Some risk analysis tools do not average the value of future losses but calculate single occurrence losses (SOL). An SOL is the estimate of the loss which occurs from a single occurrence of a threat and does not depend upon the rate of occurrence. Still other tools claim to be "expert systems" with security intelligence built into them to derive a body of both facts and speculative data.

The qualitative approach takes the point of view that many potential losses are intangible; therefore, risks cannot be easily specified monetarily. Risk results are portrayed in a linguistic manner (i.e., "no risk" to "very high risk"). Some qualitative approaches carry the risk result a step further, where risk is represented mathematically as a scalar value (i.e., a value from one to five, or one to ten, etc.) with descriptive terminology for each point on the scale. Still others provide graphic decision tree illustrations which provide a probability distribution highlighting common causes.

3.1.3 Output Results

Another important consideration of any risk analysis tool is the results it brings. Some tools do not address safeguard selection, while some do an extensive job. For example, some risk analysis tools include a complete and iterative safeguard evaluation process, whereas others do not consider it.

Some tools consider the costs of safeguards and their return on investment (ROI). The benefit of implementing cost-effective safeguards is estimated by calculating the difference in dollars between the loss impact and the cost of the security safeguard over the system life cycle. If the cost of the safeguard is less then the expected loss, then the safeguard is considered cost-effective.

Safeguard selection is clearly a useful feature of any risk analysis tool, but it may not always be within the scope of the tool. The important point is that the risk analysis tool should provide managers with a good understanding of where to apply limited dollars to protect vital computer assets.

3.2 Site-Specific Selection Criteria

Any risk analysis tool, whether used to analyze a computer facility or an application, should satisfy the principles described in the previous sections. In addition, site-specific selection criteria should be developed and used to evaluate each product being considered. The information provided in this section may be used to develop site-specific requirements. The generic requirements criteria presented here include:

- o Hardware and software requirements
- o Methodology
- o Reporting
- o Documentation
- o History and security features
- o Utility and ease of use
- o Training and technical support
- o Cost

An overview of the features and capabilities of tools currently in use is included in each category.

3.2.1 Hardware and Software Compatibility

It is cost-beneficial to select a risk analysis tool that will process on computer hardware commonly in place at the organization rather than procuring special computers. Peripheral hardware requirements should also be determined (i.e., color monitor, graphics, plotter, or modem) along with operating system requirements. The inability of any automated risk analysis tool to meet hardware and software requirements should result in reconsideration of the tool or in updating current equipment.

Summary of Capabilities:

Currently, only one risk analysis tool requires a mainframe computer; all others require microcomputers. Memory requirements range from 64K bytes of memory to 256KB of RAM memory. Most tools require a hard disk for storage of programs and data. The source code ordinarily is not available; however, some vendors will tailor the product to meet the needs of the organization. Automated risk analysis tools are written in a number of programming languages, but this generally is not important to the user since most product vendors will not provide the source code.

3.2.2 Methodology

The methodology is the principle step in the entire risk analysis process as it seeks to determine losses that result from harmful events. Losses are derived by either mathematical or linguistic models. The argument for justifying quantitative risk analysis that cost-effective safeguards cannot be evaluated against losses unless the risks are quantified. Conversely, quantitative methods have been criticized for forcing precise estimates even in cases where there is no reliable input data. Qualitative methodologies often emphasize descriptions rather than calculations.

As emphasized in section 3.1.2, there are numerous risk analysis methodologies from which to choose and no solution is clearly best. A risk analysis tool should not be judged solely on the basis of how quickly it produces results. Instead, the merit of a risk analysis tool is in its ability to produce correct results with a reasonable amount of effort. The tool selected should be one that allows the user to develop an understanding of how the results were reached and how they can be applied and relied upon.

Summary of Capabilities

Most risk analysis tools perform either a quantitative or qualitative analysis, while a few combine both. Some are designed to handle the analysis of large integrated information systems while others evaluate smaller, stand-alone systems.

3.2.3 Reporting Requirements

Informed and judicious decisions by management in selecting and implementing effective safeguards will depend in part on how well the results of the analysis are reported. At the very least, the reports should summarize risks or vulnerabilities and recommend safeguards for corrective action. While not mandatory, a list of recommended safeguards is desirable; items should be prioritized and based upon mandatory security requirements and expected savings in loss reduction or cost/benefit ratio.

Summary of Capabilities:

The quality of reports varies with each risk analysis tool. Some tools produce inclusive reports that are useful to management while others produce reports that are practical as supporting documentation. Some tools produce asset inventory lists, threats/vulnerabilities lists, ALE reports, safeguards selection details, cost benefit analysis, matrices of threats and vulnerabilities. Some plot risk results in graphic representation allowing the user to quickly compare risks from different threats. Several risk analysis tools allow the user to select, and in some cases to modify, specific reports from a variety produced.

3.2.4 Documentation

Comprehensive documentation associated with the software is essential to ensuring effective use of the tool. The documentation should provide information that thoroughly explains the operation of the risk analysis tool, instructions for loading, explanations of error messages, and re-execution instructions.

Summary of Capabilities:

Generally, user manuals are provided with the purchase of an automated risk analysis tool. The quality of the documentation may vary from one tool to another requiring the need for careful examination.

3.2.5 History and Security Features

Since the information gathered about a computer system or application is highly sensitive, requirements for security controls should be determined (i.e., logon password or encryption capability). The ability to identify participants in the risk analysis is useful if questions should arise later. An ability to maintain the information collected during data collection may also be useful in future analyses. At a minimum, it should be possible to collect the following information:

- o Participants in the analysis
- o Date of entry
- o Date of modifications, additions and deletions

Summary of Capabilities:

Many risk analysis tools have minimal security controls built into the software. While security controls in a risk analysis tool are not absolutely necessary, they could be of added benefit. If security controls are not a feature of the tool selected, it will be necessary to follow procedures that will ensure the protection of highly sensitive information collected about the organization.

3.2.6 Utility and Ease of Use

The ability to effectively and easily use a risk analysis tool is an important consideration. The tool which is difficult or cumbersome to operate will not be used. Before purchasing a risk analysis tool, all requirements should be defined and submitted to the developer. A demonstration of the tool will ensure these requirements are met. In addition, evaluations from current users will confirm the capabilities of the product.

Summary of Capabilities:

Many risk analysis tools are menu-driven with online help facilities. Some tools provide user menus which access questionnaires, calculations, reports, and system installation procedures. Some use full-screen, interactive data entry and include database management and word processing functions. Several risk analysis tools allow the user to develop report formats and questionnaires. Several product developers offer demonstration diskettes to further facilitate understanding of the tool.

3.2.7 Training and Technical Support

Effective use of any risk analysis tool depends, in part, on the training of the analysts who will use it. Therefore, detailed guidance and training should be an inherent consideration when selecting a tool.

Summary of Capabilities:

Training and technical support are generally available for risk analysis tools. Some product vendors include training with the cost of purchase; others provide ongoing support via telephone (sometimes referred to as "hotline" support); still others provide onsite training. Some vendors provide consulting services as well. The amount of support provided in some cases depends upon the license purchased.

3.2.8 Cost

Understanding all fees involved with using risk analysis tools is an important consideration in selection. These fees often include cost of multiple copies of the software, training, and installations. Costs alone should not dictate the choice of an automated risk analysis tool, however. The methodology, types of reports, quality of documentation, ease of use, and support and services offered by the vendor should be heavily weighed.

Summary of Capabilities:

Basic costs associated with the purchase of automated risk analysis tools include:

- o licensing fees
- o maintenance and installation fees
- o software updates
- o training fees
- o consulting services

3.3 Summary

This section has described the fundamental elements of a risk analysis tool along with the requirements for developing evaluation criteria. Capabilities of risk analysis tools currently in use were summarized at the end of each discussion.

APPENDIX A
THE SELECTION PROCESS

The process for selecting a risk analysis tool is similar to that for other software acquisitions. The entire process can be performed in a few steps:

1. Assign personnel to evaluate the tools
2. Define requirements criteria as discussed in section 3.2.
3. Prepare selection checklist
4. Request demonstration of the candidate packages
5. Evaluate the alternatives
6. Select a package(s)

The most favorable approach to evaluating risk analysis tools is to have a team of specialists evaluate the product. Since this is unlikely in most organizations, the next best approach is to have at least one person who has knowledge of risk analysis requirements to evaluate candidate tools. The worst approach is to assign on an ad hoc basis someone who has little experience or interest in risk management and information security.

When an organization is considering a risk analysis tool, the product evaluator must define the requirements of the organization and identify products which satisfy these requirements. A demonstration of an automated risk analysis product can verify that the tool meets mandatory requirements, and validation with present users can provide confirmation.

The capabilities of any risk analysis tool must meet site-specific requirements. The checklist contained here follows the specifications presented in section 3 and provides examples of questions that may be used in the evaluation process. The answers to these questions can be separated into high, medium, and low priority items:

Hardware and Software Compatibility

Is the minimum hardware configuration compatible with the requirements of the organization?

Can the tool be readily modified to operate on other hardware configurations?

Is the operating system the same as that utilized by the user?

Methodology

Is there a description of the underlying methodology?

Is the methodology based on mathematical principles?

Does the methodology support the policy of the organization?

Does the tool examine physical, environmental, procedural, and human interaction with the computer system being analyzed?

Does the methodology support both qualitative and quantitative results?

Nature of Results

Are the results of the analysis well presented?

Are the reports comprehensive?

Are the reports useful?

Does the tool rank the results in priority order (e.g., from high to low)?

Does the tool provide advice for safeguard selection?

Does the tool provide iterative safeguard selection?

Does the tool provide cost benefit analysis?

Utility and Ease of Use

Is the tool user-friendly?

Does the tool offer useful options (e.g., data management routines, on-line help facility, etc.)?

Documentation

Is there a manual describing the tool in over-all terms?

Is the documentation thorough?

Is the documentation easy to use and maintain?

Will the documentation be kept up-to-date by the developer?

Does the documentation meet the organization's standards?

Security Features

Does the tool document participants in the analysis?

Does the tool control access to risk analysis data (e.g., logon/password encryption)?

Does the tool provide an audit capability?

Training and Technical Support

Is installation support provided?

Is on-site training available?

Is training in usage of the tool provided as part of the installation support?

Will the developer provide future maintenance and ongoing product support?

Does the developer have the personnel and financial resources to provide adequate product support?

Enhancements

Does the developer plan further enhancements to the product?

What is the cost for providing future system enhancements?

Will the developer provide modifications to the product if requested?

Cost

What services are provided as part of the basic purchase price?

Installation
Licensing
Training
Maintenance
Modifications
Software Updates

Is there a charge for multi-installation usage?

RISK ANALYSIS TOOLS SELECTION CHECKLIST

NAME OF RISK ANALYSIS TOOL_____

CAPABILITIES	WEIGHT FACTOR	COMMENTS
METHODOLOGY:		
Quantitative Only		
Qualitative Only		
Both Quantitative and Qualitative		
DATA COLLECTION CAPABILITY:		
Assets		
Threat Sources		
Vulnerabilities		
Safeguards Evaluation Effectiveness		
UTILITY:		
Ease of Use		
Menu-Driven		
On-Line Help Facility		
Error Messages		
Reiterative Safeguard Selection		
Quality of Documentation		
Training		
SECURITY CONTROLS:		
Logon/Password		
Encryption		
History file of analysis		
REPORTING CAPABILITIES		
Safeguard selection		
Safeguard Cost/Benefit Analysis		
Management Oriented Format		
Graphic Representations		
Detail Narrative		
Print/Display Full Report		
Print/Display Loss Analysis		
Cover Pages		
Table of Contents		
Page Headers/Footers		
PRODUCT SUPPORT:		
On-Site Training Available		
Installation Support		
Telephone Support		
Scheduled Enhancements		

APPENDIX B
REFERENCES

The following list of documents, publications, and organizations provide a wide variety of information on varying aspects of risk management and risk analysis. The list is not intended to be all-inclusive, rather it is meant to serve as a starting point for those interested in learning more about risk management and risk analysis.

BROW88 Browne, P., Laverty, J.E., Using Decision Analysis to Estimate Computer Security Risk, Proceedings, Computer Security Risk Management Model Builder's Workshop, Denver, CO, May 1988.

CARR84 Carroll, J.M., Managing Risk: A Computer-Aided Strategy, Stoneham, MA; Butterworth Publishers, 1984.

DESC88 Characteristics of Automated Risk Analysis Tools, prepared by the National Institute of Standards and Technology, January 1989.

FIPS65 Guidelines for Automatic Data Processing Risk Analysis; National Bureau of Standards; August 1969.

FIPS31 Guidelines for Automatic Data Processing Physical Security and Risk Management; National Bureau of Standards; June 1974.

FIPS87 Guidelines for ADP Contingency Planning; National Bureau of Standards; March 1981.

GUAR88 Guarro, S., Analytical and Decision Models of the Livermore Risk Analysis Methodology (LRAM), Proceedings, Computer Security Risk Management Model Builder's Workshop, Denver, CO., May 1988

HOFF86 Hoffman, L., Risk Analysis and Computer Security: Bridging the Cultural Gap, Proceedings, 9th National Computer Security Conference, sponsored by the National Bureau of Standards and the National Computer Security Center, September 15-18, 1986.

HOFF88 Hoffman, L., A Prototype Implementation of a General, Risk Model, Proceedings, Computer Security Risk Management Model Builder's Workshop, Denver, CO., May 1988.

JACO88 Jacobson, R., IST/RAMP and CRITI-CALC: Risk Management Tools, Proceedings, Computer Security Risk Management Model Builder's Workshop, Denver, CO., May 1988.

KATZ88 Katzke, S., A Government Perspective on Risk Management of Automated Information Systems, Proceedings, Computer Security Risk Management Model Builder's Workshop, Denver, CO., May 1988.

LEWI89 Lewis, N., Kemmerer, R., Risk Analysis Tool Comparison Framework, Proceedings, Computer Security Risk Management Model Builder's Workshop, Ottawa, Canada, May 1989.

MAYE88 Mayerfeld, H., Definition and Identification of Assets as the Basis for Risk Management, Proceedings, Computer Security Risk Management Model Builder's Workshop, Denver, CO., May 1988.

MOSL88 Mosleh, A., A Matrix/Bayesian Approach to Risk Management of Information Systems, Proceedings, Computer Security Risk Management Model Builder's Workshop, Denver, CO., May 1988.

OMB130 OMB Circular No. A-130, Management of Federal Information Resources, December 1985.

OTWE89 Otwell, K., Aldridge, B., The Role of Vulnerability in Risk Management, Proceedings, Computer Security Risk Management Model Builder's Workshop, Ottawa, Canada, May 1989.

PARK81 Parker, D.B. Managers Guide to Computer Security, Reston Publishing, 1981.

SMIT88 Smith, S., LAVA: An Expert System Framework for Risk Analysis, Proceedings, Computer Security Risk Management Model Builder's Workshop, Denver, CO., May 1988.

SNOW88 Snow, D., A General Model for the Management of ADP Systems, Proceedings, Computer Security Risk Management Model Builder's Workshop, Denver, CO., May 1988.

SP500-85 Executive Guide to ADP Contingency Planning; National Bureau of Standards; January 1982; NBS Special Publication 500-85.

SP500-109 Overview of Computer Security Certification and Accreditation; National Bureau of Standards; April 1984; NBS Special Publication 500-109.

SP500-133 Technology Assessment: Methods for Measuring the Level of Computer Security, National Bureau of Standards; October 1985; NBS Special Publication 500-133.

SP500-134 Guide on Selecting Backup Processing Alternatives; National Bureau of Standards; November 1985; NBS Special Publication 500-134.

SP500-153 Guide to Auditing for Controls and Security: A System Development Life Cycle Approach; National Bureau of Standards; April 1988; NBS Special Publication 500-133.

WHIT88 White, G., Mate, K.V., Air Force Experience with PC-Based Risk Analysis Systems; Proceedings, Computer Security Risk Management Model Builder's Workshop; Denver, CO., May 1988.

☆ U.S.GOVERNMENT PRINTING OFFICE : 1989-261-013-00077

NBS-114A (REV. 2-8C)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET (See instructions)	1. PUBLICATION OR REPORT NO. NIST/SP-500/174	2. Performing Organ. Report No.	3. Publication Date October 1989

4. TITLE AND SUBTITLE

Guide for Selecting Automated Risk Analysis Tools

5. AUTHOR(S)

Irene E. Gilbert

6. PERFORMING ORGANIZATION (If joint or other than NBS, see instructions)

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
(formerly NATIONAL BUREAU OF STANDARDS)
U.S. DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered

Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

Same as item # 6

10. SUPPLEMENTARY NOTES

Library of Congress Catalog Card Number: 89-600769

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)

This publication is intended to assist in the selection of appropriate automated risk analysis tools. It contains information that will be helpful in developing requirements evaluation criteria.

12. KEY WORDS (Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)

computer security; risk analysis; risk management

13. AVAILABILITY

☒ Unlimited

☐ For Official Distribution. Do Not Release to NTIS

☒ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

☐ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES

34

15. Price

USCOMM-DC 6043-P80

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SYSTEMS TECHNOLOGY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published quarterly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW., Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards and Technology
(formerly National Bureau of Standards)
Gaithersburg, MD 20899