RISKTOOL.TXT

RISK MANAGEMENT RESEARCH LABORATORY OVERVIEW

The National Institute of Standards and Technology (NIST) and the National Computer Security Center (NCSC) have cooperatively established a Risk Management Research Laboratory located at the NIST facilities in Gaithersburg, MD.

The primary objective of the laboratory is to conduct research in risk management techniques and methodologies. As part of this endeavor, risk management software products will be surveyed to determine their applicability to different agency environments. A demonstration capability is also planned. Although official product evaluations will not be conducted, reports outlining the characteristics and capabilities of products surveyed will be prepared.

An additional goal of the laboratory is to develop and publish guidance on currently available risk management methods. We plan to develop a "standard" test case for use in the laboratory. The test case will provide a focal point for controlled analysis and documentation. It is further planned to develop data on computer security incidents for estimating threat frequencies, vulnerabilities, losses, direct and indirect impacts, etc.

A longer range goal of the laboratory is to develop and validate a formal framework for analyzing, developing, and implementing risk management methods. We will be looking for methods of risk management which could be economically employed across a broad spectrum of computer environments and upon which standards could be based. It is intended that workshops will be organized to evaluate current and future technology for this purpose.

Technical contributions and comments are welcome from interested parties from both the public and private sectors. The point of contact for the laboratory is Irene Gilbert (NIST), (301) 975-3360.

Application Control Matrix

Methodology. Matrix approach. This methodology presents application controls, control objectives, and risks in a mate format. The matrix provides a summary of the security environment which allows the user and auditor to quickly view where added safeguards are needed. A data base of controls from which to make selections is included in this software package.

Hardware Requirements.

- IBM PC or compatible.

- Two diskette drives or one diskette drive and a fixed drive.

Operating System.

- MS-DOS Version 2.0 or later.

Laser Interface~ease of Use.

- Menu-driven.
- Online HELP facility.

Documentation and Training.

- User Manual.

Developer/Vendor. Nander Brown & Co., Reston, VA (202) 653-6646.
Remarks.
Government agencies may obtain copies of this software at no charge.

BDSS (Bayesian Decision Support System).

Methodology. Quantitative/Qualitative. BDSS is programmed to gather tangible and intangible asset valuation data and to ask questions that assess potential risks using quantitative data bases provided by the vendor. The user can include site-specific threat experiences which the algorithms will process along with the quantitative knowledge base. Threats, vulnerabilities, asset categories, and selected safeguards are automatically mapped and cross-mapped to each other. system ranks threats before and after the implementation of safeguards so that the representation of comparable exposure to loss may be examined. The analysis results are typically displayed graphically with risk curves based on dollar loss values and probability of loss coordinates. The central algorithms of BDSS are based on Bayes' Theorem addressing uncertainty and statistical methods. BDSS software produces a variety of printed reports as well as ASCII files that may be exported to the user's word processor. The vulnerability analysis feature of the BDSS application also provides a stand-alone qualitative presentation of safeguard system weaknesses.

Hardware requirements.

- IBM PC/AT or compatible.
- 640KB memory.
- 20MB fixed drive and one diskette drive.
- Graphics card (CGA/EGA)

Operating System.

- MS-DOS Version 3.0 or later.

User Interface/Ease of Use.

- Menu driven.

Documentation and Training:

- User manual.
- Training is not included with purchase but may be provided upon request.

Developer/Vendor. Ozier, Perry & Associates developed BDSS in a joint venture with Pickard, Lowe and Garrick, Inc. of Newport Beach, CA and Washington, DC. For further information regarding the software contact Ozier, Perry & Associates, San Francisco, CA; (415) 989-9092

Remarks. BUDDY SYSTEM

Methodology. Qualitative. The Buddy System is an automated risk analysis methodology for microcomputer environments and comprises two components: (1) countermeasures survey and (2) security analysis and management (SAM). This software package assesses the level of vulnerability based on safeguards already in place. The level of information being processed on the system determines whether or not the assessed level of vulnerability is acceptable. Recommendations for corrective action are provided for each vulnerability that falls outside of the acceptable range through the use of on-line "what if' scenarios. A data base containing over 100 safeguards is included in this software package. Further, the Risk Management component of the system allows the analyst to track recommended corrective action implementations for reports and/or follow-up procedures.

Hardware Requirements.

- IBM PC or compatible.
- 256KB memory.
- 10MB fixed drive and one 360K diskette drive.

Operating system.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- On-line HELP facility.

Documentation and Training.

- User manual.

- One-day on-site training course.
- Training component built into the software to increase security awareness.

Developer/Vendor: Countermeasures, Inc., Hollywood, MD; (301) 373-5166.

Remarks.

- Optional Maintenance Utility allows the user to customize the software.
- Report and screen formats can be edited with standard DOS editor.

CONTROL MATRIX METHODOLOGY FOR MICROCOMPUTERS

Methodology. Matrix approach. This software provides a matrix approach for designing controls into microcomputer system environments. It identifies which controls are necessary to ensure adequate security in business or scientific systems. The software package contains four separate systems.

Package 1 (Designing Controls into Computerized Systems) is an educational tool that teaches the user how to design and develop a control matrix.

Package 2 (Risk Ranking the Matrix) teaches the use of Delphi and Comparison Risk Ranking techniques to rank threats and their controls.

Package 3 (Automated PC-Based Control Matrix Design) is a control matrix development package that contains a database of controls plus separate databases of threats and computer system components. This package allows one to draw a draft matrix, search the controls database and move relevant controls to a matrix controls list.

Package 4 (Show Text Presentation Graphics) is used to draw the final matrix resequencing threats, components, and controls.

Hardware Requirements.

- IBM PC or compatible or IBM Personal System/2.
- 384KB memory.
- Two diskette drives or 10MB fixed disk.
- Graphics capability.

Operating system.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- A demo diskette provides a ten minute introduction to the matrix concept of designing controls into computerized systems.

Documentation and Training.

- User manual.
- Automated course.
- One or two day on-site training upon request.

Developer/Vendor. Jerry Fitzgerald & Associates, Redwood City, CA (415) 591-5676

Remarks.

CRAMM (CCTA Risk Analysis and Management Methodology)

Methodology: Qualitative. CRAMM is a risk analysis tool developed by the British government and BIS Applied Systems Limited. CRAMM is composed of three stages, each supported by questionnaires and guidelines. The primary function of Stage 1 is the valuation of data and physical assets of the system or network under review. Qualitative values are determined for the data assets on a scale of 1 to 10, for potential impacts of disclosure, modification, destruction, and availability. The physical asset are valued on the basis of replacement costs, which are also convened to scalar values of 1 to 10, with 10 representing the highest value. The review moves to stage 2 for those assets valued higher than 3. (Baseline protective measures are recommended for assets valued lower than 3).

Stage 2 measures the levels of threats and vulnerabilities for each asset group and then measures the risks on a scale of 1 to 5. In stage 3, these measures are used to select safeguards from a library of over 900. CRAMM provides an iterative safeguard evaluation, in priority sequence, to facilitate selection of the most appropriate safeguards. A variety of reports are produced. CRAMM also provides a password logon function. Sensitivity markings are provided on all screens and hardcopy output.

Hardware Requirements.

- IBM PC or compatible.
- 640KB memory.
- 10MB fixed drive.

Operating System.

- MS-DOS 2.1 or later.

User Interface/Ease of Use.

- Menu-driven.
- On-line HELP facility.

Documentation and Training.

- User manual.
- Management guide.
- Training available upon request.

Developer/Vendor. BIS Applied Systems Limited, London SE1 9PN, England; telephone 011-44-1-633-0866.

Remarks. CRAMM is available in the USA by licence agreement between BIS and the UK Central Computer Telecommunications Agency. The BIS Service Representative and provider of a US-based help desk and support services is Executive Resources Associates, Inc., Suite 813, One Crystal Drive, Arlington, VA 22202; (703) 920-5200. CRITI-CALC

Methodology: Quantitative/Qualitative. This product uses the concept of annualized loss expectancy (ALE) to quantify the criticality of risk exposure for applications. The software collects information about each application's loss potential, optimum off-site recovery, cost of backup, cost 10 recover. It uses this information to calculate each application's annualized risk potential. The criticality of each application is determined by the potential for loss caused by a processing interruption and a profile of up to 14 delay factors. The user interacts with the system by means of screens which display information about the risk exposure. Once the user has reviewed the initial results, "what if" analysis may be performed by modifying the input data as a way of verifying the effectiveness of certain safeguards. The information contained in the output reports may be used to optimize contingency plans. The ALE, as a function of maximum outage duration, is compared with the corresponding cost of backup data to identify automatically the optimum off-site recovery site.

Hardware requirements:

- IBM PC/XT or compatible.
- 64OK memory.
- 360K diskette drive.
- Feed drive not necessary but convenient.

Operating SYstem:

- MS-DOS Version 2.11 or later.

User Interface ease of Use:

- Menu-driven.
- Help screen.

Documentation and Training:

- User manual with sample databases and detailed tutorial.
- On-site training.

Developer/Vendor: International Security Technology, Reston, VA (703) 471-0885.

Remarks.

GRA/SYS

Methodology. Qualitative. GRA/SYS is a tool designed to assist internal auditors and security personnel in developing a work priority plan for reviewing organizational risks. Specifically, the software prepares an applications and computer activity inventory, determines the number of risks for several major control areas. A risk score that reflects the measure of risk to the organization is calculated and placed in descending order on a scale of 1 to 9, with 9 representing a worst-case situation. An additional report that reflects the number of times each risk occurs is also prepared. Using the output reports from this software package, the user is able to identify those risks where more effective safeguards are needed.

Hardware Requirements.

- IBM PC or compatible.
- 64KB memory.
- One diskette drive.

Software Requirements.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.

- Training is not offered with the purchase.

Developer/Vendor. Nander Brown & Co., Reston, VA.;
(202) 653-6646.

Remarks.

Government organizations may obtain this software at no cost.
IST/RAMP (International Security Technology/Risk Analysis Management Program)

Methodology. Quantitative and Qualitative. 1ST/RAMP is a mainframe-resident risk analysis program with an input module that is PC-resident. The software calculates the annualized loss expectancy and as well as single occurrence loss. The system can also provide a qualitative analysis. 1ST/RAMP generates data collection forms to assist the risk analyst in organizing and controlling data collection. Five loss categories are addressed: service interruptions; physical loss and damage; fraud; unauthorized disclosure; and physical theft. A library of data bases enables the analyst to maintain an audit trail of input data changes. A 'what-if' capability enables the analyst to select the most cost-effective security measures.

RAMP<->LINK~is a PC-resident, menu-driven data entry system which uses risk information entered by the analyst to build a DOS file that can be uploaded to IST/RAMP for processing.

Hardware Requirements.

- IBM Mainframe for IST/RAMP--30xx with MVS.
- Interactive under TSO and Roscoe.
- IBM PC/XT or compatible for RAMP<->Link.
- 5K12 memory.
- Two diskette drives or one diskette and fixed disk drives.

Software Requirements.

- MS DOS Version 2.1 or later.

User Interface/lEase of Use.

- Menu-driven.

Documentation and Training.

- Training manual with sample data bases and detailed tutorial.
- User manual.

- Three-day on-site training.
- Pocket reference.

Developer/Vendor International Security Technology, Reston, VA; (703) 471-0885.

Remarks.

RAMP<->L~ makes it unnecessary for the analyst to be familiar with the details of 1ST/RAMP data entry formats. The analyst enters the data off-line and logs onto a mainframe where 1ST/RAMP is resident using any communications software package that has a "file send" command.

JANBER

Methodology: Qualitative. Janber initiates a yes/no questionnaire and checklIst for collecting information about security controls already in place. The software weights safeguards currently in place and measures them against the level of data being processed on the system. These data classification levels point to highly sensitive but unclassified information to highly classified data. The analysis provides a linguistic characterization of the level of vulnerability from 2-28, with 28 representing a worst-case scenario. Vulnerabilities, safeguards and their weights can be preestablished by the vendor to meet the organization requirements. Safeguards that are required but not implemented are flagged in a report and recommendations for safeguards that meet organizational guidelines and directives are provided. Users have the capability of performing "what-if' scenarios to evaluate the effectiveness of certain safeguards.

The Janber application allows users to define standard entries for specific data fields. The results of the data collection and analysis are maintained on separate data bases. The developer recommends that both the analysis and the data collection be performed by different personnel to assure the integrity of the results. The developer further recommends that the analysis be performed by computer security professionals to achieve optimum results. The software provides a capability to track action items resulting from the evaluation.

Janber creates a database of information on all systems surveyed and provides a data base query capability for contingency planning and recovery operations.

Hardware Requirements.

- IBM PC or compatible.
- 10MB Feed drive and one diskette drive.

Operating system.

- MS-DOS Version 2.0 or higher.

User Interface/Ease of Use.

- Menu-driven.
- On-line help facility.

Documentation and Training.

- User manual.
- Training provided upon request.

Developer/Vendor. Eagan, McAIlister Associates, Inc., Lexington Park, MD 20653; (301) 862-3565.

Remarks. LAVA (Los Alamos Vulnerability and Risk Assessment)

Methodology: Qualitative and Quantitative. LAVA administers questionnaires which results in the identification of missing safeguards in 34 areas ranging from password management to personnel security and internal audit practices. The software evaluates potential consequences and impact upon the organization and the ultimate loss exposure (risks). LAVA considers three kinds of threats: natural and environmental hazards; accidental and intentional on-site human threats (including the authorized insider); and off-site human threats. Detailed LAVA reports provide both qualitative and quantitative results of the risks identified.

Hardware requirements.

- IBM PC- or compatible.
- 512KB memory.
- 360KB and 720KB diskette drives; or 1.2MB fixed drive and one 360~ diskette drive.

Operating System.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Interactive questionnaires.

Documentation and Training.

- User manual.

- On-site training.
- Demonstration diskette.

Developer/Vendor. Los AIamos National Laboratory, Los AIamos, NM; (505) 667-7777.

Remarks.

The LAVA methodology stresses a team approach for conducting the risk assessment. It is recommended the team be composed of people with a broad spectrum of backgrounds and expertise to ensure a thorough assessment. It is further recommended that a consensus among the group be reached before entering an answer to any of the questions, and that in some cases this may be the most difficult part of administering this risk management software.

Distribution of this package is handled through the National Security Agency (contacts include Sam Samuelson (301)~688-6022; Ed Markel (301) 688-6022; or John LaPaille (301) 688-5331.

LRAM (Livermore Risk Analysis Methodology)

Methodology: Quantitative. A government-developed system, this methodology is structured to allow screening of asset/threat-event combinations so that only high impact risks are reviewed. The methodology focuses attention on the effectiveness of proposed security controls as well as those already in place. LRAM is divided into three major phases to include project planning, risk analysis, and decision support. The initial phase defines the scope of the analysis and identifies needed resources and personnel. The second phase analyzes the data collected from phase 1. In this second phase, risk elements are identified by establishing corresponding threats, control and asset components, the results of which are provided as input for the final decision support phase.

The final decision support phase is meant to assist in the security management of information. It is a process to select and list in priority order each recommended safeguard on the basis of cost benefit estimates and other decision indexes.

Hardware Requirements.

- IBM PC or compatible.
- 640K memory.
- One diskette drive and fixed drive.

Operating SYstem.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.

Developer/Vendor~ Lawrence Livermore National Laboratory, Livermore, CA; (415) 423-3083 or 543-3082.

Remarks.

MARION

Methodology. Qualitative/Quantitative. LION assesses business risks associated with information systems drawing on a large database of actual incidents. The software incorporates a questionnaire to evaluate the level of security that is currently being applied within the organization. Each question is allocated a weighting which reflects the relative importance according to the analysis of the underlying database of events. A score is allocated for each question; the responses and scores are stored. The software calculates the overall score for 27 categories of security and presents the results graphically and in printed form. Once the current security profile has been determined, MARION compares each category with industry norms which are derived from the database. The software uses the information on costs also held iii the database to calculate an estimated expenditure in relation to the total security budget. The calculated costs are analyzed according to the nature of the security category and presented graphically in detailed tables. A "what-if" capability allows one to use different budgets to determine the effects on the security profile. The effects of the proposed measures can also be displayed.

Hardware Requirements.

- IBM PC or compatible.
- 5l2K memory.
- Graphics capability.

Operating System.

- MS DOS 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User Manual.

Developer/Vendor. Coopers & Lybrand (United Kingdom firm), Plumtree Court, London EC4A 4HT, telephone 01-822-4678.

Remarks.

MARION is a methodology developed in France. Coopers & Lybrand are the agents for the package in the UK. They have worked with a French software house PSI to produce an English version of the package and supporting reference material.

MicroSecure Self Assessment

Methodology. Qualitative. An automated software tool that will allow PC users to conduct a security self-assessment. The software analyzes the PC environment, determines the vulnerabilities, and recommends security controls. Those safeguards recommended are designed to increase security and reduce exposures in six areas to include system integrity, data security, credibility, data integrity, backup and disaster recovery, and confidentiality and privacy. The software may be customized to meet specific requirements.

Hardware Requirements.

- IBM PC or compatible.
- 256K memory.
- One diskette drive.

Operating System.

- MS DOS 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User Guide.
- On-line tutorial.

Developer/Vendor Boden Associates, East Williston, NY; (516) 294-2648.

Remarks. An optional question quiz is provided at the end of each chapter of the training course. Recommendations for corrective action can be printed directly to the printer or written to an ASCII text file for editing.

MINIRISK

Methodology. Qualitative. MINIRISK is a tool designed to assess computer security vulnerabilities in a micro computer environment. A vulnerability assessment questionnaire allows the organization to evaluate the adequacy and completeness of individual safeguards areas and to reevaluate these same areas after missing safeguards have been implemented. During the process of answering the MINIRlSK questionnaire, the user identifies missing safeguards in 10 to 50 vulnerability categories ranging from password management to contingency planning and internal audit controls. Safeguards and controls considered mandatory by the organization have been appointed for each category that is to be reviewed. The absence of certain safeguards determines the level of vulnerability on a scale of zero to 9, with zero being the best case, and 9 the worst. MINIRISK establishes a threshold by which to evaluate vulnerabilities that exceed an acceptable risk level.

Hardware Requirements.

- IBM PC or compatible.
- 64KB memory.
- One diskette drive.

Software Requirements.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.
- Online HELP facility.
- User defined questionnaire.

Documentation and Training.

- User manual.
- Training is not offered with the purchase.

Developer/Vendor. Nander Brown & Co., Reston, VA.; (703) 689-4580.

Remarks. Government organizations may obtain this software at no

cost.

PRISM Risk Analysis and Simulation for the PC

Methodology. Qualitative. Prism supports development of risk analysis modelling, simulation, sensitivity analysis, and graphical presentation of results. It also contains system functions to save, retrieve, display, and modify existing models. In addition to simple algebraic equations, Prism permits use of BASIC-like statements to model more complex applications.

Hardware Requirements.

- IBM PC or compatible.
- 512K fixed drive.

Operating System.

- MS-DOS 2.0 or later.

User Interface/lEase of Use.

- On-line HELP facility.

Documentation and Training.

- User manual.
- Training and on-site seminars.
- Consulting services available to assist in model development.

Developer/Vendor. Palisade Corporation, Newfield, NY;
(607) 564-9993.

Remarks.

QUICKRISK

Methodology: Qualitative. Quikrisk requires the user to input information about the systems and facilities on a scenario form. These forms pertain to potential threats, current safeguards, and assets. Once all of the input information has been entered, the software computes the results which provide an annual loss exposure. An additional computation is performed which displays a return on investment for each control in place. The analyst also has the capability of modifying the results of previous computations by modifying the input data. In addition, the software is delivered with a threat file containing numerous threats and frequencies. The user has the capability of adding threats to this list.

Hardware requirements.

- IBM PC or compatible.
- Two diskette drives.

Operating System.

- MS-DOS Version 2.0 or later.

User Interface~se of Use.

- Menu-driven.

Documentation and Training.

- User manual.

Developer/Vendor Basic Data Systems, Rockville, MD;
(301) 269-2691.

Remarks.

RANK-IT

Methodology. RANK-IT is a risk assessment software package that uses the Delphi technique. Delphi is an expert system approach to risk ranking. This software automates the Delphi technique by adding Comparison Risk Ranking to obtain an ordinally ranked list of the items being ranked or to calculate percentage risk values. Each ranked item has a numerical value that can be used as a weighting factor or a cardinal number value.

RANK-IT is used to risk rank system threats, controls, vulnerabilities, components, or any other criteria. It also can be used to rank other types of business decision alternatives, whether quantifiable or not.

The developer suggests that the time required to conduct a risk ranking using this combined Delphi and Comparison Risk Ranking methodology can range from 30 minutes to three hours.

Hardware Requirements.

- IBM PC/XT/AT or compatible or IBM Personal System/2.
- 5l2KB memory.
- Single diskette drive or fixed disk (300K memory required).
- Graphics capability.

Operating System.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- Demonstration diskette.
- User manual.
- Tutorial and training diskettes.
- One-day on-site training upon request.

Developer/Vendor. Jerry Fitzgerald & Associates, Redwood City, CA; (415) 591-5676.

Remarks.

Risk Analysis System (RA/SYS)

Methodology. Quantitative. RA/SYS is an automated risk analysis system which processes with a series of interconnected files that can assess up to 50 vulnerabilities and assets and 65 threats. Calculations are performed on threat/vulnerability pairs to produce threat ratings and threat frequencies. A report summarizes loss estimates, cost benefit analysis, and return on investment.

Hardware Requirements.

- IBM PC or compatible.
- 128KB of memory.
- Two 360KB diskette drives or 640KB fixed drive.

Operating System.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.
- On-line HELP facility.

Documentation and Training.

- User manual.
- Technical assistance available upon request.

Developer/Vendor Nander Brown & Co., Reston, VA; (202) 689-4580.

Remarks.

Government agencies may obtain copies of this software at no charge.

RiskCALC

Methodology. Quantitative or Qualitative. An annual loss expectancy (ALE) or other metric is computed based on an answered questionnaire. The user may optionally change the values of RiskCALC variables to determine the most cost-effective safeguards and display the results on the user's screen. RiskCALC is part of a 'family' of software tools described below. They each provide a standard ASClI file interface for exporting and importing RiskCALC variables.

o RiskCALC allows the user to answer questions and print reports into which values elicited from the questionnaire are automatically inserted.

o Risk Minimizer identifies an organization's most significant risks from a completed analysis. Risk Minimizer may be used with other risk management software tools that use the RiskCalc file format.

0 The System Manager assists in designing or customizing an existing risk analysis model.

o The Demonstration Models allow the user to develop a site-speciiic questionnaire or select one that models several risk scenarios.

Hardware requirements.

- IBM PC or compatible.
- 5I2KB memory.
- Fixed drive is optional but recommended.

Operating system.

MS-DOS Version 2.1 or later.

User Interface/Ease of Use.

- Menu driven.
- On-line help facility.
- Lotus-like iriterface.

Documentation and Training.

- User and system administrator manuals.
- One day on-site training with purchase.
- A three-day course on computer security and risk management is available upon request.

Developer/Vendor. Hoffman Business Associates, Inc., Chevy Chase, MD., (301) 656-6205.

Remarks

RISKPAC

Methodology. Qualitative. This software product is composed of three components--questionnaire, surveys, and reports. The results of the questionnaire are stored in a 'survey' which provides the basis of the analysis. The questions point to discrete categories that provide a review of an organization's policies, physical environment, processing hardware and the applications and data which make up a system. Each of these categories are evaluated separately. A variety of questionnaires that apply to several disciplines (e.g., manufacturing, banking, and government) are available. 'Reports' provide the results of the evaluation expressed on a scale of one to five, with five representing a worst-case scenario. The weighting and scoring algorithms are based on Kepner/Tregoe type of analysis. The package can produce data files that can be input to various database spread sheets. Further, the software is equipped with a number of utility routines that allow organizations to develop their own questionnaires. This 'System Manager' capability is available separately.

Hardware Requirements.

- IBM PC, PC/XT, or PC/AT or compatible.
  256K ofmemory.
- Two diskette drives or 10MB fixed drive.

Operating system.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.
- Training provided upon request.

Developer/Vendor: Computer Security Consultants, Ridgefield, CT,

Subsidiary of Computer Security Consultants, LTD.; (203) 431-8720.

Remarks.

RISKWATCH

Methodology. Qualitative/Quantitative. The RISKWATCH software is capable of analyzing organizations, facilities, systems, applications and networks, both large and small. RiskWatch distinguishes between financial, critical, sensitive and classified systems. The system access relational data bases that contain over thousands of relationships between threats, assets, vulnerabilities, losses, and safeguards. Responses to a questionnaire which addresses a wide variety of job functions is combined with the databases to produce a comprehensive risk analysis report. This report also provides an asset inventory, a detailed list of vulnerabilities, threat analysis with annual loss expectancies and recommended safeguards that include return-on-investment. The system provides a query capability for any selected threat, asset, vulnerability or safeguard.

Hardware requirements.

- IBM-XT/AT or compatible.
- 640K memory.
- 10MB fixed drive.
- Graphics.
- Color monitor.

Operating system.

- MS DOS Version 2.1 or higher.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.
- Training provided upon request.

Developer/Vendor. Expert Systems Software, Inc., Long Beach, CA (213) 499-3346.

Remarks.

The software can be customized to meet the needs of both defense and civil organizations. LOGICON is authorized to distribute this software package, Arlington, VA (703) 486-3500.