386

Work Priority Scheme for EDP Audit and Computer Security Review

Zella G. Ruthberg

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Institute for Computer Sciences and Technology
Gaithersburg, MD 20899

and

Bonnie T. Fisher

Department of Health & Human Services
Office of Inspector General
Washington, DC 20201

March 1986

Issued August 1986

DEPARTMENT OF COMMERCE
DNAL BUREAU OF STANDARDS

NBSIR 86-3386

WORK PRIORITY SCHEME FOR EDP AUDIT AND COMPUTER SECURITY REVIEW

Zella G. Ruthberg

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Institute for Computer Sciences and Technology
Gaithersburg, MD 20899

and

Bonnie Fischer

Department of Health & Human Services
Office of Inspector General
Washington, DC 20202

March 1986

Issued August 1986

U.S. DEPARTMENT OF COMMERCE, Malcolm Baldrige, *Secretary*
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Director*

WORK PRIORITY SCHEME FOR EDP AUDIT AND COMPUTER SECURITY REVIEW

Editors:

Zella G. Ruthberg
Institute for Computer Sciences and Technology
National Bureau of Standards

and

Bonnie T. Fisher
Department of Health & Human Services
Office of Inspector General

March 1986

TABLE OF CONTENTS

FIGURES

TABLES

ABSTRACT

This report describes a high level risk analysis for Automated Information Systems (AISs) that can be used by computer security reviewers and EDP auditors to prioritize their non-discretionary and discretionary review activities for these AISs. It divides the risk analysis problem into five areas of risk concern (called dimensions) with each area defined by a set of characteristics. The five dimensions are: Criticality/Mission Impact, Size/Scale/Complexity, Environment/Stability, Reliability/Integrity, and Technology Integration. The report presents two possible two-level risk scoring schemes, each of which calculates the level of risk for each dimension, uses the Criticality score as a first order system risk score, and then combines all five dimension risk scores for a second order system risk score. One scoring method is simple and intuitive; the other scoring method is more detailed. An approach for deriving an EDP audit or computer security review plan using these scores is outlined.

KEYWORDS

audit/review plan
automated information system risk analysis
computer security review
Criticality/Mission Impact
discretionary audit/review
EDP audit
Environment/Stability
non-discretionary audit/review
Reliability/Integrity
risk score
Size/Scale/Complexity
Technology Integration

1. INTRODUCTION

1.1 The Work Priority Scheme in Perspective

This report describes a methodology for prioritizing the work to be performed by EDP Auditors and Computer Security Reviewers. It is based largely on the results of a Spring 1985 public/private sector workshop of EDP auditors and systems developers who explored the criteria for assessing risk in computer systems. The workshop was co-sponsored by NBS and the EDP Systems Review and Security Work Group of the President's Council on Integrity and Efficiency (PCIE). The Work Group was established in October of 1983 under the auspices of the PCIE Computer Security Project, chaired by Richard P. Kusserow, Inspector General (IG) of the Department of Health and Human Services (HHS). (See Appendix A for membership in and further description of the Work Group.) The methodology described in this report is to be included in the EDP system development audit guide currently being developed by this Work Group for joint publication by the PCIE and the National Bureau of Standards (NBS).

1.2 Internal Controls and Security Safeguards

Although it may at first appear strange to have the same methodology applicable to both EDP audit and computer security review, further analysis of these two activities reveals the similarity of their focus. EDP audit is concerned with the review of internal controls in an Automated Information System (AIS), while Computer Security review examines the security safeguards in an AIS. Security must be recognized as only one, albeit a major category of internal controls. A study performed by Arthur Young for the Department of Energy [1], recognized that computer security controls are a <u>subset</u> of the internal controls to be found in an AIS. The major difference between these two sets of controls is that internal controls address efficiency and effectiveness <u>in addition to</u> security issues. The Office of Management and Budget, in their OMB Circular A-130 (a re-write of OMB Circular A-71 TM1 (Computer Security)), acknowledges the interrelationship between internal control and security concerns in both their definition of key terms and their acceptance of internal control reviews and documentation in lieu of security reviews. OMB Circular A-123 also reflects this correlation.

1.3 Brief Overview of the Scheme

The Scheme described in this report enables its user to systematically perform a risk-based evaluation of the subjects for EDP audit/security review within an organization (i.e., the universe of its AISs), and to arrive at a risk measurement for each AIS. This final risk measure (or score) is based on an analysis of risk in key areas of concern (dimensions for describing risk) in that system. These scores enable the user to rank the systems by determining which AISs offer the highest levels of risk to the organization and which dimensions within each AIS contribute most to this high level of risk. Based on this analysis, the user can then draw up an EDP audit or security review work plan for the organization in question. The work plan would include annual coverage along with a basis for formulating the scope of specific AIS reviews. Considering the generality of the dimensions and their associated characteristics, the scheme is equally appropriate for public and private sector review subjects.

The scheme employs a two-level review and the characteristics associated with the five dimensions. The levels for the dimensions are:

Level I
  Criticality/Mission Impact

Level II
  Size/Scale/Complexity
  Environment/Stability
  Reliability/Integrity
  Technology Integration

Each dimension is defined by a related set of characteristics which are used to estimate or calculate the amount of risk posed by that dimension to the failure of the system. A Level I review looks at Criticality/Mission Impact of the system to the organization and develops a risk score for each AIS with respect to this dimension. Since this dimension is the most important of the five risk areas, it can be used as a first approximation to a system risk score. The AISs can then be placed in sequence from high to low risk and the low risk systems eliminated from further review consideration. Organizations with very limited resources could stop at a Level I review and plan their work based on these results.

To refine the risk scores further, the high criticality risk AISs are reviewed at Level II. Risk scores are obtained for the four remaining dimensions for each high criticality risk AIS. These four dimension risk scores are summed and added to the Level I risk score to yield the system risk score for that AIS. The AISs reviewed at Level II can then again be placed in sequence from high to low risk and thus enable the reviewer to prioritize his work.

Two possible risk scoring methods are suggested and described briefly in Section 4 and in detail in Appendix D. The first is a simple intuitive approach based on a minimal collection of information on the AIS; the second is more elaborate and is based on more detailed information on the AIS. Organizations with limited resources could use the simple scoring method to obtain system risk scores while those with more resources could use the more elaborate approach.

2. THE NEED FOR THE SCHEME

2.1 Dependence on Computers

As part of the Fiscal Year 1986 budget, the President highlighted systems management as one of the Federal Government's major initiatives for FY 1986 and beyond [2]. The Federal Government continues to develop 90 percent of its software, which constitutes the controlling mechanism for the approximately $14 billion spent annually on information technology. More than 120,000 federal employees are involved in programming and managing the resultant systems which will ultimately control and distribute the almost $1 trillion dollars in outlays projected for 1986. Obviously, the Federal commitment to the computer hardware, software, and management arenas has reached gigantic proportions with no tapering off in sight of either the size or the growth rate.

2.2 EDP Audits/Security Reviews - A Form of Control

In the past ten years there has been a slowly growing recognition of the need for controls in the Federal Government's automated systems. Although there often is resistance among program sponsors or user management to employing internal controls within AISs because of the cost, time, and overhead that such controls can introduce, the interest in and use of controls in AISs is continuing to grow. This growth is augmented by the increasing emphasis OMB has placed on internal controls since the passage of PL97-255, the Federal Managers' Financial Integrity Act of 1982 [3], and the completion and revision of their own Circular A-123. (See Section 2.3 for descriptions of these control requirements.) The General Accounting Office (GAO), at Congressional request, has closely followed the Federal agencies' implementation of A-123, and, thus far, has been dissatisfied with agencies' compliance--especially in the area of internal controls in AISs.

Internal audit organizations, whose activities existed long before the computer age, have long recognized and stressed the need for internal controls in manual (primarily financial) systems and the need for independent audits as a critical component of the oversight of an organization's systems. With the advent of computerized AISs in organizations, career fields specializing in EDP audit (generally found in audit organizations) and security review (often found in audit or management) have developed. Recognition and revision of their role in the review of automated systems is continuing, and increasing rapidly.

2.3 Formal Requirements for Audits and Reviews

The major legal requirements for EDP audits and security reviews within Federal agencies are found in three OMB circulars: A-130, A-123, and A-127. Circular A-130 (the follow-on to A-71

TM1) outlines specific requirements for establishing agency security programs, and specifies the use of (1) design reviews and system tests for security during development of applications (to be used for certification of application) (2) periodic security audits or reviews of applications for recertification, and (3) periodic risk analyses of installations. OMB Circular A-123, issued in 1981 and revised in 1983, outlines for Federal agencies specific policies and standards for establishing and maintaining internal controls in their programs and administrative activities. This includes requirements for vulnerability assessments and internal control reviews. The main provisions of A-123 were made into law through the enactment of the Federal Managers' Financial Integrity Act of 1982. OMB Circular A-127, issued in 1984, outlines for Federal agencies specific policies and standards for establishing and maintaining internal controls in financial management systems. This includes requirements for annual reviews of agency financial systems which build on reviews required by OMB Circular A-123. In addition to these three key legal directives, internal audit and security are subject to departmental requirements, audit organization recommendations, and GAO audit standards for computer based systems [4].

2.4 Size of Review Task

A major implication of the enormous numbers of computers and our dependence on them, found today in government (see section 2.1) as well as the private sector, is that the universe of AISs that need reviewing is also enormous. However, the number of trained EDP auditors and security reviewers to do this job has not kept pace with the size of this problem. A consistent methodology for obtaining a risk score for an AIS is seen as a major tool for culling through the review work that needs to be done and assigning relevant as well as realistic workloads to the review staff available within an organization.

3. BACKGROUND ON THE METHODOLOGY

3.1 The Invitational Workshop

The PCIE Work Group, in the course of its activities, decided that an essential component of their final product, Guide to Auditing for Controls and Security Throughout the Systems Development Life Cycle, was a methodology for prioritizing the EDP auditor's work. Rather than rely exclusively on the experience and background of the Work Group members, it was decided to hold an invitational workshop on the subject and use the ideas generated during the course of the workshop to develop a work priority scheme.

The 2 1/2 day workshop was held in March of 1985. A "strawman" scheme (see Appendix B), used as a starting point for discussions, was provided by William Perry, based on a Harvard Business Review article [5] by F. Warren McFarlan on predicting the failure of systems under development. The 62 attendees included EDP auditors, senior ADP managers, and computer security specialists from both the Federal Government and the private sector. (See Appendix C for list of attendees.) Presentations, to set the stage, were given on the first morning by attendees from Coopers & Lybrand, Touche Ross & Co., General Motors, International Security Technology Inc., and Management & Computer Services, Inc. The attendees were then divided into five discussion groups, each of which had 1 1/2 days to analyze the "strawman" and come up with their own version of a work priority scheme, based on the "strawman" framework of providing critical risk dimensions with associated characteristics. Each group presented its scheme at the closing session of the workshop.

3.2 Workshop Points of Agreement

Although each group came up with a somewhat different set of major audit/security concerns (dimensions) for the scheme, there was universal agreement on four underlying premises:

1. The entire EDP audit plan[1] must first give consideration to non-discretionary audits (mandated by law, regulation, and/or the agency/organization management). These are reflected in the front end qualifiers. Only if there are remaining resources for EDP audit would the scheme be used as originally intended.

2. The risk based prioritizing evaluation needs to be performed at two levels, Level I and Level II.

3. The first level of inquiry (for its Level I dimension) should concern itself with the criticality of the AIS to the agency/organization mission. Only critical systems should be reviewed further (for its Level II dimensions[2]) and given a more detailed risk score.

4. The ranking and rating of the risk characteristics of each dimension is program and agency/organization specific. Only the risk scoring method is applicable across the board.

[1]) It should be understood that the terms EDP audit and security review may be used interchangeably throughout the scheme and the surrounding discussion.

[2]) The four major concerns or dimensions to be addressed in a Level II review (presented in section 4.4) are a synthesis of the conclusions drawn by the five workshop discussion groups. Two analysis approaches for risk measurement (or scoring) are discussed briefly in Section 4.6 and in detail in Appendix D.

4. A WORK PRIORITY SCHEME FOR THE EDP AUDITOR

4.1 Assumptions and Caveats

The use of the proposed work prioritizing scheme is based on certain ideal assumptions and caveats. These include:

- An inventory of all computer systems (AISs)--operational, under development, or undergoing major change--is maintained, to establish the audit universe.
- The above inventory may not be complete due to user development or system changes made outside the system development process.
- To use the priority scheme, certain minimal information is required or the assessment of the system may not be valid.
- The full priority scheme would most easily be performed by EDP audit groups in order to enlist multiple perspectives, especially where resources are known to be a concern.
- Auditors in the organization must agree that risk can be evaluated by a standardized scheme.
- Users should always be consulted in the risk evaluation conducted by the auditor to ensure appropriate assumptions, and to assure maximum effectiveness.
- Auditor judgement is still needed!

Within this framework of assumptions and caveats the entire EDP audit work plan can then be developed. To the degree these assumptions differ from the reality of the organization's SDLC environment, the work planning methodology should be adjusted.

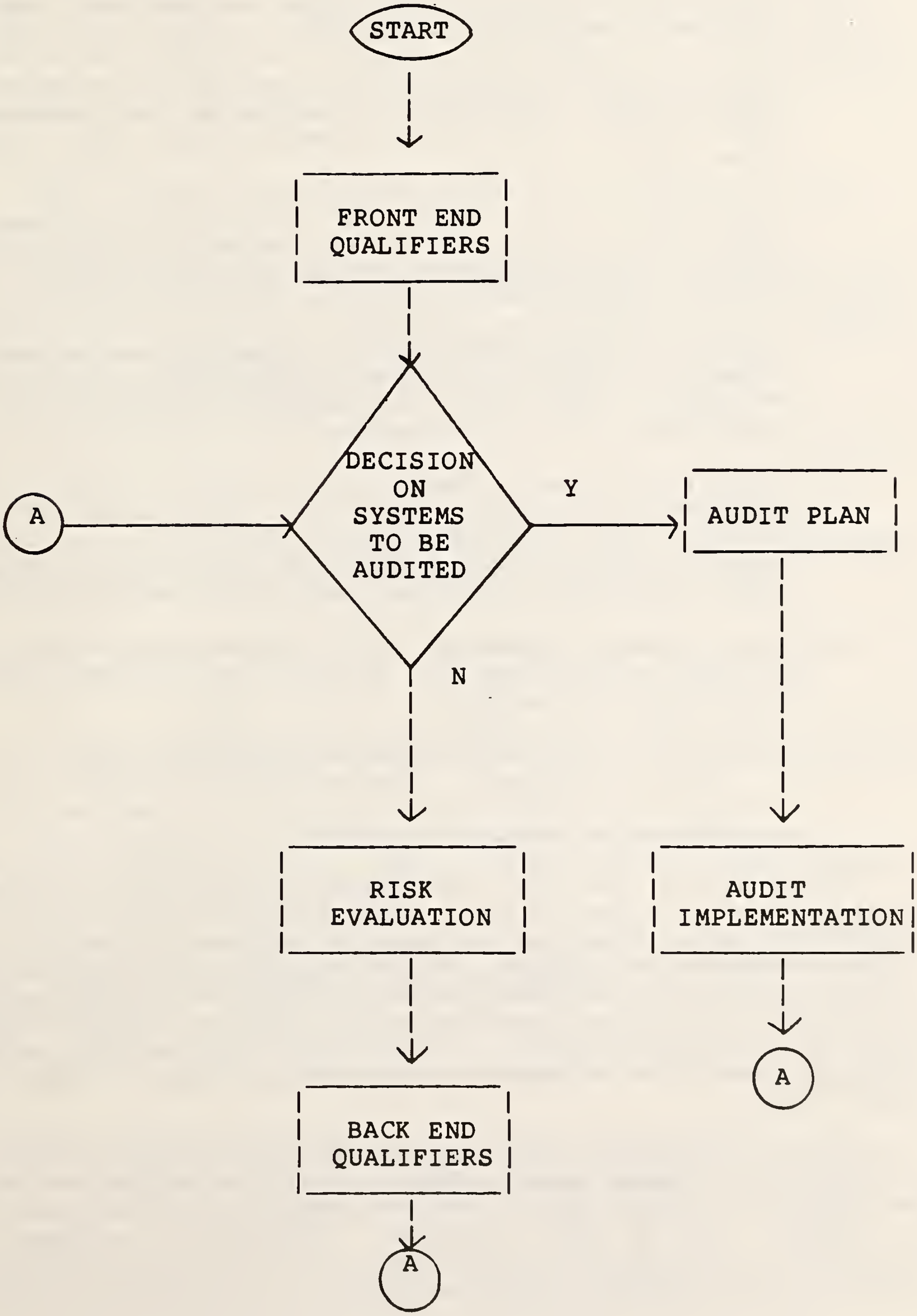
4.2 Audit Planning/Prioritization Process

The risk evaluation performed as part of the work priority scheme must be done within the context of the entire audit planning process. There are elements of the process that need to be considered prior to the risk evaluation (such as non-discretionary audit requirements) and other elements that require consideration afterwards (such as resource constraints). The following sections contain a suggested model for the entire prioritization process.

4.3 Non-Discretionary Audits

As can be seen from the model in Figure 1, the audit planning and prioritization process starts with front end

Figure 1 AUDIT PLANNING/PRIORITIZATION PROCESS



qualifiers that must be considered by the auditor prior to making decisions with respect to which system(s) should be audited. These front end qualifiers consist of nondiscretionary factors which are beyond the auditor's control. These nondiscretionary factors include, but are not limited to the following:

- External directives (e.g., laws, regulations, OMB circulars, and audit standards);
- Internal directives and priorities (e.g., contractual requirements; requirements, standards, and policies of audit and data processing organizations; upper management directives);
- Business/organizational environment unique to the organization (e.g., effect of economy on organization, budget of organization, and technology available to or used by organization);
- Organizational unique factors (e.g., presence and strength of quality assurance and security functions, management and control philosophy, structure, and policies);
- Geo-political environment (e.g., public concern and politics);
- Resource constraints/economic health (e.g., dollars, time, expertise, training, tools, and techniques);
- Known problems with the system, from current logs or previous evaluations and audits (e.g., nature and magnitude of problems);
- Evaluations and audits planned by management;
- Auditor's institutional knowledge of organization's universe of systems.

After all of the front end qualifiers have been considered, it may be that the entire audit plan is dictated by the nondiscretionary work. That is, external directives, internal directives, business environment, unique organization/responsibilities, and/or resource constraints may require that certain audits be performed and these required audits may use up the limited audit resources available. In this case, the priority scheme may still be useful for determining audit approaches and where to focus efforts.

If, on the other hand, additional audit resources are available for discretionary audits, the risk evaluation of the work priority scheme can be used to identify and rank the systems in greatest need of audit coverage. Ultimately, back end qualifiers may need to be considered for the discretionary audits, as described in Section 5.

4.4 Risk Evaluation Levels and Dimensions

The work priority scheme expresses the risk concerns in terms of two levels and five dimensions. The risk concerns in Level I are reviewed first and those in Level II are reviewed second. Level I has one dimension and Level II has four dimensions. Each dimension is defined as a related set of characteristics which can estimate or measure the amount of risk posed by that dimension to a failure of the system. The chief concern of each dimension can be stated in the form of a question as follows:

1. What is the impact/criticality of the system to the organization?

A poorly developed or controlled system that is mission critical could jeopardize an organization's basic operational or programmatic effectiveness; therefore, an impact/critical system commands audit attention. The larger the impact, the more important it is to audit.

2. How complex is the system? (This includes size considerations.)

The more complex the system, the more difficult is communication and control, and consequently, the higher the risk of failure. The greater the chance for failure, the more important it is to audit the system.

3. How stable is the system internally (structure) and externally (environment)?

The less stable the system, the more difficult it is to develop procedures for communication and control, the greater the chance for failure, and the greater the need to audit.

4. How reliable is the system and the information it processes and generates (i.e., what is the chance of the system failing or the data being wrong)?

The answer to this question is obtained by looking at the controls in the system (integrity controls) and prior audit experience. The less reliable, the more chance for failure and the need to audit.

5. How well is the technology integrated into the organization?

The poorer the system technology is integrated with the skills of the staff and the standards and procedures of the organization, the more chance for failure and the greater the need to audit.

These questions serve as the basis for the five dimensions and their associated characteristics developed for the work prioritization scheme. Identified simply the two levels and five dimensions are:

Level I
1. Criticality/Mission Impact

Level II
2. Size/Scale/Complexity
3. Environment/Stability
4. Reliability/Integrity
5. Technology Integration

The five workshop discussion groups believed strongly that the overriding dimension of the five should be Criticality/Mission Impact. Systems that significantly impact the mission of an organization, or key organizational components, would easily take precedence over all other dimensions in allocating EDP audit resources. Because Criticality/Mission Impact was such an overriding dimension, the work priority scheme was developed as a two level scheme. Level I is composed of the dimension Criticality/Mission Impact while Level II is composed of the remaining four dimensions: Size/Scale/Complexity, Environment/Stability, Reliability/Integrity, and Technology Integration.

The two level work priority scheme permits a high amount of flexibility depending on organizational need since it can be applied in any degree of detail required. For example, the results of Level I ranking may be adequate to prioritize all audit work, based on available time and resources. If additional ranking characteristics are necessary, the more detailed Level II can be used to further prioritize audit work. A two level review, additionally, enables the auditor to purge from consideration those systems which will definitely not be reviewed, for any number of reasons. Environment and resource issues enter in here.

The two level work priority scheme follows in outline form, identifying the five dimensions and their related characteristics. [Note that the same characteristic may be used in more than one dimension because the question asked will be different.]

4.5 Two Level Work Priority Dimensions/Characteristics

4.5.1 Level I:

A. <u>Mission Impact/Strategic Value/Organization (Business) Criticality and Sensitivity Factors</u>

- o criticality of system to organization mission
- o criticality/sensitivity of system to well being, safety or interest of general public/clients/consumers

- criticality/sensitivity of data and information
  - competitive advantage
  - confidence of public in program/department
  - privacy/confidentiality/security issues

- materiality of resources controlled by system

- fraud potential

- life cycle costs of system (people and dollars)
  - development cost budget
    - people
    - dollars
      - hardware
      - software
      - facilities
  - operating cost budget
    - people
      - data processing/systems (including training)
      - users (including training)
    - dollars
      - hardware (CPU, peripherals, terminals, telecommunications, etc.)
        - acquisition
        - operation
      - software
        - acquisition
        - maintenance
      - supplies
      - facilities
      - configuration change control

- degree of dependence on AIS

- criticality of interfaces with other systems and external organizations

A Level I review, outlined above, provides a "first cut" at the total audit universe. This initial review will identify critical systems that require audit coverage. The additional dimensions to be reviewed in Level II should be used to rank these critical systems to find those most deserving of discretionary audit coverage.

4.5.2 Level II:

B. System[3] Size/Scale/Complexity

[3] The term "system" is used in place of "project" to signify the entire AIS life cycle and the possibility of auditing at any point in the development process or operations.

- o size of user area impacted
- o number/complexity of interfaces/relationships with other projects or systems
- o complexity of AIS technology (e.g., network size, communication needs, system configuration, degree of centralization, nature of transaction coupling mechanisms, nature of security)
- o size/complexity of system
  - size of system budget
    - . development costs
    - . maintenance/operation costs
  - number/complexity of different inputs
  - number/complexity of unique files
  - number/complexity of unique outputs
  - number/complexity of logical files (views) system will access
  - number/complexity of major types of on-line inquiry
  - number of source documents maintained/retained
  - number/complexity of computer programs
  - complexity of programming language
  - complexity of system configuration
  - number of human elements interfacing
  - number of decision levels
  - number of functions by devices
  - number, types and complexity of transactions
  - number of external organizations impacted
- o nature of interactions with external organizations

C. <u>System Environment/Stability</u>

- o organizational breadth (interfaces, dependencies, system configuration)
- o management involvement/commitment
- o project management approach and structure
  - configuration management program
  - management efficiency and effectiveness
- o specificity of, agreement on, and support for user requirements
- o confidence in estimates -- both cost and time -- premising make-or-buy decisions, vendor selection, system testing/validation, etc.
- o number of vendors/contractors involved

- newness of function/process to user

- problems associated with current system performance and/or system development effort

- existence/scope of data processing standards, policies and procedures, especially systems development life cycle methodology and documentation requirements

- availability of evidence - document and report preparation and maintenance for entire systems life cycle (e.g., test/validation/certification results, operations manual, system specifications, audit trails, exception reporting)

- quality and completeness of documentation

- general controls
  - physical access controls
  - environmental controls
  - communication controls
  - management controls environment
  - document controls
  - system change and test/validation/certification controls

- on-going concern issues/organization effect (will mission objectives be met in a timely manner?)
  - interruption tolerance
  - ability to maintain performance
  - unsatisfactory system performance (adverse consequences from degradation or failure)
  - unsatisfactory system development completion
  - unsatisfactory conversion

- labor relations (e.g., salary parity, hours, fringe benefits, etc.)

- project team (management and staff effectiveness and training)

- organizational and personnel changes (frequency, magnitude and number)

- functional requirements changes (frequency, number, and magnitude)

- technical changes (e.g., frequency, magnitude and number)

- factors affecting cost/economic/budget climate

- availability and adequacy of back-up and recovery procedures

D. Reliability/Integrity

- hazards/risks to information system (data, hardware, communications, facilities)
- general controls
  - environmental (e.g., physical access controls, natural hazards controls)
  - management
- applications controls
- availability and adequacy of audit trails
- quality and quantity of automated error detection/correction procedures
- availability and adequacy of back-up and recovery procedures
- completeness, currency and accuracy of documentation for audit
- prior reviews (e.g., A-123, A-127, A-130, audits--internal, CPA, QA--IRM triennial reviews)
- auditor judgement (intuitively obvious)

E. Technology Integration

- make-up of project team in relation to technology used (number, training, and experience)
- applicability of the data processing design methodologies and standards to the technology in use
- pioneering aspects (newness of technology and/or technological approaches used in this information system for application and organization)
- technical complexity of information system (interrelationships of tasks)
- user knowledge of DP technology
- margin for error (i.e., is there reasonable time to make adjustments, corrections or perform analyses before the transaction is completed?)
- utilization of equipment (tolerance for expansion)
- availability of automated error detection/correction procedures

- completeness, currency and accuracy of documentation for implementation/maintenance/operation (e.g., operations/maintenance manuals).

- amount of hardcopy evidence

4.6 Risk Scoring -- Application of the Work Priority Scheme

4.6.1 Implementation of the Scheme

For the scheme to be of use to the EDP auditor, an analysis approach for risk scoring must be employed using the dimensions and characteristics. Two possible approaches for arriving at a system risk score are suggested here and described in Appendix D. The first scoring method is a simple intuitive approach based on a minimal collection of information on the AIS while the second one is more elaborate and based on more detailed information on the AIS. User experience will undoubtedly lead to modifications and improvements in the application of the scheme and the risk scoring methods. If the EDP reviewer for some reason does not wish to use a scoring methodology, he/she could still keep the dimensions and their characteristics in mind when performing a less formal review.

4.6.2 A Simple Scoring Approach

The simple approach assigns a weight and a risk level to each dimension, based on a qualitative judgement with respect to the characteristics associated with each dimension. Criticality/ Mission Impact is always assigned the highest weight. The product of the weight and risk level of a dimension is the risk score for that dimension. The Criticality/Mission Impact risk score is then the Level I system risk score. To obtain the Level II system risk score, the sum of the dimension risk scores over the four Level II dimensions is added to the Level I system risk score. (See Appendix D for details.)

4.6.3 A Detailed Scoring Approach

The more detailed approach looks in depth at the characteristics associated with each dimension. Each dimension is defined by a set of characteristics which are used to calculate the amount of risk posed by that dimension to the failure of the system. Each characteristic is given a weight and a risk level. The product of these two numbers is the risk score of the characteristic and the sum over the risk scores of the characteristics of a dimension yields the dimension risk score. Again, the Criticality/Mission Impact risk score is the Level I system risk score. And again, to obtain the Level II system risk score, the sum of the dimension risk scores over the four Level II dimensions is added to the Level I system risk score. (See Appendix D for details.)

5. Discretionary Audits

After the systems have been identified and ranked, using the risk based evaluation, several back end qualifiers must be considered by the auditor in determining how many discretionary audits can be added to the audit plan (See Figure 1). These back end qualifiers can be categorized in two areas:

- Audit Types and Objectives, and

- Audit Resource Constraints

Figure 2 identifies the different audit methodologies that can be used and the different audit objectives that can be accomplished in performing ADP audits. The auditor must consider the audit methodology to be performed and the audit objective to be accomplished in deciding on the number of additional (discretionary) audits that can be performed. Furthermore, these issues must be considered in light of the audit resource constraints (e.g., people, time, dollars, expertise) that exist. For example, to perform a system under development audit which looks at security, confidentiality, and privacy issues requires substantially more resources than an operational system audit which looks at only data reliability issues. Thus, the mix of audit methodologies to be performed, and the existing audit resource constraints must be considered when deciding on the number of discretionary audits that can be added to the audit plan. After these back end qualifiers have been considered, the audit plan can then be finalized, and audits implemented.

6. USES OF THE WORK PRIORITY SCHEME

The risk scores developed during the risk based evaluation can be used for both developmental and operational systems. The major difference between risk based evaluations of these two classes of systems is that (1) the ranking of characteristics may change, and (2) some characteristics may not even be applicable to both. The following is a brief enumeration of some possible uses of the Work Priority Scheme (from "strawman" scheme in Appendix B).

1) To determine relative risk between applications - A risk score of one application is compared to scores developed for other applications in the same department. Thus, risk scoring is used to determine relative risk among applications. The score is not used to determine an absolute measure of risk.

2) To create an audit risk profile - An audit risk profile is a pictorial representation of the various risk characteristics measured. While the audit risk score shows audit risk for the entire automated information system, the risk profile shows the relational risk among the various risk characteristics. The objective of the risk profile is to graphically illustrate what characteristics contribute to the total risk, and in what proportion.

Figure 2 AUDIT AREAS OF CONCERN*

	OBJECTIVES				
METHODOLOGY	Data Reliability	Security Confidentiality Privacy	Availability of Information Resources	Efficiency Economy Effectiveness	Compliance
(A) System Development Life Cycle Process					
(B) System Under Development					
(C) Operational Systems (Post Implementation)					
(D) Function, e.g., Management, Teleprocessing, Data Processing					

* Decisions on audit methodology and objectives desired will influence:
- Weights given when ranking risk factors
- Audit scope, i.e., level of involvement (e.g., tasks, dollars, hours)

3) To modify the characteristics contributing to audit risk - Both the auditor and data processing management can use the audit risk scheme to identify those characteristics which may cause the information system to be less successful than proposed. For example, if the application project personnel do not understand the computer technology being used, the probability of success of the information system being developed diminishes. Once the characteristics that may cause the system to be less successful than desired are known, those characteristics can be altered such that the probability of the system being successful increases.

4) To help allocate audit resources - The information gathered during the audit risk analysis can be used as a basis for allocating audit resources to review application systems and/or review specific aspects of those systems. For example, high-risk information systems may receive extensive reviews, medium risk cursory reviews, and low risk no reviews. For those systems reviewed, the area of review can be selected based on the high-risk characteristics. For example, if computer technology is a high-risk characteristic, the auditors may want to expend time reviewing how effectively the project team is using that technology.

5) To develop a data base of risk characteristics - The information gathered during this process should be saved and used for two purposes. The first use is to improve the audit risk prioritization scheme to make it more predictive of audit risk; and the second use is to assist data processing management in structuring and planning projects such that those projects will have the highest probability of success.

7. PROBLEMS WITH AND SOLUTIONS TO USE OF SCHEME

Potential difficulties in using the work priority scheme and methods for overcoming these difficulties were discussed by the PCIE Work Group participants in order to facilitate the use of the scheme. These follow in outline form.

7.1 Potential Difficulties in Utilization

- Time and resources needed for sufficient data collection

- Inadequate organization data processing planning

- Need to establish an understanding of and agreement on related issues on a consistent basis by all affected parties (auditors/systems developers/users/etc.)

- Need to convince affected management (audit and opera tions) as to the credibility of scheme and its impact on audit coverage, given a finite level of audit resources

- Initial time and resources needed to adapt the work priority scheme to the organization

- Represents a snapshot at a given point in time which requires maintenance and updating to ensure its continued validity

- Need for audit planning to be separate from and sensitive to data processing and business cycle planning processes

- Requires integrated skill knowledge that includes relevant expertise in pertinent specialty areas

- Work priority scheme just another tool for audit manage ment to consider in its decision-making process

- EDP audit resources still likely to be insufficient to provide coverage suggested by scheme

- Requires up-to-date and complete inventory of AISs--all those which are operational, developmental, and undergo ing change

7.2 Methods for Overcoming Difficulties

- Make underlying questionnaire and data gathering methods as simple as possible for administering it.

- Refine data collection methods through experience and learning curve.

- Educate users (including DP community) regarding needs for standards, planning, etc..

- Audit recommendations should emphasize necessary improvements to DP and business executives.

- Encourage early participation and collective editing to reach consensus on data collection instrument.

- Apply retroactively to existent systems to demonstrate the risks that audit coverage would have addressed.

- Emphasize that initial commitment would have long-term benefits; and that once established, maintenance would be considerably less costly.

- Analyze dynamics of the organization and the audit component within it to determine the frequency of "snapshot". Workload mix and control attributes may be affected accordingly.

- Use means for staying attuned to planning cycles.

- Consider supplementing EDP audit resources with financial and generalist auditors for areas not requiring specific technical expertise. They may even be more relevant for business and institutional knowledge.

- EDP audit resources may be supplemented with consultants for areas requiring highly skilled data processing specialists.

8. Recommendations

The workshop attendees came up with a number of recommendations for further activity in this crucial EDP audit area. A brief enumeration of these follows.

1) The work priority scheme described here should be tested within organizations by applying it to the EDP planning considerations of a prior year's workload universe. This might help ascertain how EDP audit resources may have been allocated differently and whether that allocation may have better assisted management in identifying and overcoming resultant control deficiencies in the systems.

2) Feedback should be captured on institutional knowledge of why and how systems have failed so that one could determine whether the draft scheme would have targeted EDP audit resources on the most vulnerable systems.

3) A prototype needs to be developed which would include a survey questionnaire, a weighting and scoring system, a testing process, a methodology for evaluating results and modifying the prototype, a method for the selection of testing sites, and a method of quantifying qualitative issues that would facilitate a comprehensive cost-benefit evaluation of the work priority scheme.

References

[1.] "ADP Internal Control Guide," U.S. Department of Energy, DoE/MA-Ø165, August 1984.

[2.] Executive Office of the President, Office of Management and Budget, Management of the United States Government, Fiscal Year 1986. Washington, D.C.: U.S. Government Printing Office, 1985.

[3.] Federal Managers' Financial Integrity Act of 1982, Public Law 97-255, September 8, 1982.

[4.] "Standards for Audit of Governmental Organizations, Programs, Activities, and Functions," U.S. General Accounting Office, 1981 Revision.

[5.] "Portfolio Approach to Information Systems," F. Warren McFarlan, Harvard Business Review, September - October 1981.

APPENDIX A

PCIE WORK GROUP ON EDP SYSTEMS REVIEW AND SECURITY

SUMMARY OF BACKGROUND AND CHARGE

President Reagan established the President's Council on Integrity and Efficiency (PCIE) in March 1981 to coordinate government-wide efforts to attack fraud and waste and help ensure system integrity in government programs and operations. Chaired by the Deputy Director of the Office of Management and Budget, the Council is composed of the Inspectors General (IGs), as well as representatives from the Federal Bureau of Investigations, the Department of Justice and the Office of Personnel Management. Among its other functions, the PCIE is charged with developing interagency programs and projects to deal efficiently and effectively with those problems concerning fraud and waste which exceed the capability or jurisdiction of an individual agency.

In October 1983, the Council established a working group on Electronic Data Processing (EDP) Systems Review and Security under the leadership of the Inspector General of the Department of Health and Human Services, to be included under his ongoing Computer Security Project. Composed of IG and management representatives from 14 Federal Departments and Agencies, the group is charged with facilitating and improving Office of Inspector General/Audit organization reviews of automated information systems (AISs), particularly those systems under development. The objective of the PCIE Work Group is to improve the likelihood that auditable and properly controlled systems are being developed.

To achieve this objective, the PCIE Work Group participants drew from the Department of Defense life-cycle approach to the management of automated systems, and the National Bureau of Standards' Institute for Computer Science and Technology's (NBS/ICST's) Special Publications and Federal Information Processing Standards, to develop a system life cycle functional matrix for AISs. That matrix, structured around critical AIS documentation requirements, is intended to clarify the potential functions of the internal auditor vis-a-vis other key participants in the EDP planning, design, implementation and review processes. With the life cycle matrix as a conceptual framework, an audit guide is being developed to facilitate the successful fulfillment of that role, focusing on systems under development and major modifications to existing systems.

PCIE WORK GROUP MEMBERS

Bonnie Fisher (Project Leader)	Dep't of Health & Human Services Office of Inspector General
John Bjork	Small Business Administration Office of Inspector General
Jim Cox	Dep't of Health & Human Services Office of Inspector General
David Decker	Dep't of Housing and Urban Development Office of Inspector General
Bob Gignilliat	Dep't of Health & Human Services Office of the Assistant Secretary for Management & Budget
Mark Gillen	Department of Treasury IRS Internal Audit
Jim Hollohan	Smithsonian Institution Audit Agency
Mike Houston	Department of Defense Office of Inspector General
Doug Hunt	National Aeronautics & Space Administration Office of Inspector General
Wally Keene	Dep't of Health & Human Services Office of the Assistant Secretary for Management & Budget
John Lainhart	Department of Transportation Office of Inspector General
Jack Landers	General Services Administration Office of Information Resources Management
Bill Lee	Department of Commerce Office of Inspector General
Mac MacDonald	Veterans' Administration Office of Inspector General
Larry Martin	Department of Energy Office of ADP Management

APPENDIX B

STRAW MAN PRIORITIZING SCHEME

FOR USE BY AUDITORS lN EVALUATING

AUDIT RISK IN AUTOMATED lNFORMATlON SYSTEMS

OBJECTIVE OF "STRAW MAN" PRIORITlZING SCHEME

The prioritizing scheme outlined in this paper is proposed as a "straw man" for use by auditors in evaluating the audit risk in automated information systems. An audit risk (sometimes referred to as an exposure) is the probable unfavorable effect associated with the occurrence(s) of an undesirable event. Audit risk needs to be evaluated for two purposes. The first is to determine the need for, and amount of, audit resources that should be assigned to an automated information system; and the second is to point the auditor toward those system characteristics most susceptible to vulnerabilities. The following straw man has been developed primarily for use as a starting point for discussion by the attendees to the NBS/PCIE Work Group Invitational Workshop on "Work Priority Scheme for the EDP Auditor."

BACKGROUND INFORMATION AND ANALYSIS OF EXISTING RISK/PRIORITIZING METHODOLOGIES

Auditors traditionally use audit risk assessment methodologies to allocate audit resources and identify areas for investigation. While various organizations approach audit risk assessment from different perspectives, their chronological approach to audit risk assessment has usually gone through the following four phases or approaches (note that audit groups currently perform risk/exposure assessment using all four approaches):

- Approach 1 - Audit judgment and instinct

This has been, and is still, the most prominently used method of audit risk assessment. Using this approach, the auditor calls upon his/her personal experiences, coupled with other learning experiences and knowledge of organization mission and external mandates, in order to project those experiences, learning and knowledge to the automated information system (AIS) under review. The auditor intellectually tries to associate the AIS under review with past experience and knowledge to determine comparable characteristics in order to estimate the magnitude of the audit risk/exposure and to select specific system characteristics for investigation. While this method can be effective,it is not a transferable skill, but, rather, one which must be learned over time and is unique to each practitioner.

- Approach 2 - Dollar risk estimation using the risk formula

Risk is defined as the probability for loss. That probability is expressed through the formula "frequency of occurrence times loss per occurrence equals annual loss expectancy." The "frequency of occurrence" refers to the frequency with which a particular vulnerability (flaw in the system) may combine with a possible threat (a man-made or natural exploitation of the vulnerability). The "loss per occurrence" is then the negative impact of a threat/vulnerability pair. Audit risk based on this formula can be quantified in dollars. This can, under certain circumstances, provide the advantage of projecting, with high precision, risk exposure in terms readily understandable by non-technicians. FIPS PUB 65 is based on this risk assessment method. The disadvantages of projecting risks in dollars are that the base numbers are difficult to get (i.e., frequency of occurrence and loss per occurrence) and it may therefore imply a higher degree of precision than is realistic.

- Approach 3 - Identifying and weighting risk attributes

The attributes that cause risk/exposure to be realized have been at least partially identified. The relationship among these attributes can be specified through weighting. Using these attributes, an auditor can determine whether or not they are present in the automated information system under review, and through the accumulation of weighted scores rank automated application systems according to their relative audit risks. For example, this method can show that application A is of higher risk than application B. This method is most effective when the attributes are determined through statistical regression analysis.

- Approach 4 - Use of risk assessment software packages

Vendors have automated approaches two and three and made them commercially available. The first software package on determining dollar risk was marketed by Pansophic as PANRISK, and the first commercially available software package which used the attributes method to project risk was offered by Management and Computer Services as a package called ESTIMACS. The major advantages to the automated version are the ease of use and the opportunity with minimal effort to play "what if" strategies through varying one or more of the risk characteristics.

The ideal audit risk/exposure assessment method has not yet been developed. No current approach can guarantee the completely correct prediction of audit risk. However, approaches 2, 3, and 4 represent transferable skills, and because they have been formalized can be evaluated and proved. One characteristic of a risk assessment method that appears to be extremely important is its ease of use. The more difficult the method is to use, the less likely that an auditor will use it. Lacking a convenient structured method, the auditor will revert to approach 1 and rely on instinct and judgment to make audit decisions.

Many internal audit and data processing functions have developed a prioritizing scheme to evaluate the audit risk of automated information systems within their own organization. There appears to be much similarity among the various approaches. F. Warren McFarlan has attempted to categorize the dimensions of risk that are common to many of these in-house developed prioritizing schemes.

The Three Dimensions of Risk

F. Warren McFarlan, in a September-October 1981 Harvard Business Review article entitled "Portfolio Approach to Information Systems," identified three important dimensions which contribute to the risk exposure inherent in a project:

1) Project size - The larger it is in dollar expense, staffing levels, elapsed time, and number of departments affected by the project, the greater the risk/exposure. Multimillion-dollar projects obviously carry more risk than $50,000 projects and also, in general, affect the company more if the risk is realized. A related concern is the size of the project relative to the normal size of a systems development Group's projects. The implicit risk is usually lower on a $1 million project of a department whose average undertaking costs $2-$3 million than on a $250,000 project of a department that has never ventured a project costing more than $50,000.

2) Experience with technology - Because of the greater likelihood of unexpected technical problems, project risk increases as familiarity of the project team and the IS organization decreases with the hardware, operating systems, data base handler, and project application language. A project that has a slight risk for a leading-edge, large systems development group may have a very high risk for a smaller less technically advanced group. Yet the latter groups can reduce risk through purchase of outside skills for an undertaking involving technology that is in general commercial use.

3) Project structure - In some projects, the very nature of the task defines completely, from the moment of conceptualization, the outputs. The outputs of these projects are fixed and not subject to change during the life of the project. Such schemes are classified as highly structured. They carry much less risk than those whose outputs are more subject to the manager's judgment and hence are vulnerable to change.

An analysis of the attributes method of risk assessment appears to emphasize these three dimensions. Thus, while it is possible to divide audit risk/exposure into different dimensions, practice appears to support that there is consensus among those working with audit risk/exposure that these are important dimensions. Therefore, the straw man audit prioritizing scheme proposed for this invitational workshop will be constructed around these three dimensions.

NEED FOR AND USE OF AUDIT RISK PRIORITIZING SCHEME

Warren McFarlan, in his "Portfolio Approach to Information Systems" article, states that:

> "The typical project feasibility study covers exhaustively such topics as financial benefits, qualitative benefits, implementation costs, target milestones and completion dates, and necessary staffing levels. In precise, crisp terms, the developers of these estimates provide voluminous supporting documentation. Only rarely, however, do they deal frankly with the risk of slippage in time, cost overrun, technical shortfall, or outright failure. Rather, they deny the existence of such possibilities by ignoring them. They assume the appropriate human skills, controls, and so on, that will ensure success."

McFarlan and others have proposed that through proper analysis the auditor should be able to predict the probability of unfavorable consequences such as:

- Failure to obtain all, or even any, of the anticipated benefits
- Cost and/or schedule overruns
- Inadequate system of internal control
- Technical performance of resulting system that turns out to be significantly below estimate
- Incompatibility of the system with the selected hardware and software

The internal auditor has only limited resources to perform his mission. Good audit practices dictate that those resources be assigned to activities that offer the greatest payback to the organization. In 1977, The Institute of Internal Auditors issued the report from the research project entitled Systems Auditability and Control. A major conclusion from this project was that the most fruitful use of internal audit time would be participating in the automated information system development process. In addition, the U.S.General Accounting Office issued a standard, which in the 1981 revision was changed to a guideline, regarding auditor participation in system development. The general feeling of the PCIE Work Group, however, is that auditor participation during the System Development Life Cycle (SDLC) is vital to assuring the development of secure and auditable systems. The challenge has been first, what systems should the auditor participate in, and second, if they participate, where should they spend their review time?

The audit-risk-based prioritization scheme is developed to answer these challenges. It provides a basis for determining what systems should be reviewed, and for those systems reviewed indicates the characteristics on which audit effort should be expended.

AUDIT RISK PRIORITIZATION SCHEME

An effective audit risk prioritizing scheme has the following four parts:

1) Identification of risk dimensions - Previously defined as project size, experience with technology, and project structure.

2) Identification of risk characteristics - The attributes of an automated information system which permit the auditor to project the performance of an operational information system.

3) Analysis of the audit risk characteristics - Determines the applicability and importance of the characteristic in predicting the operational performance of the automated information system.

4) Use of the audit risk assessment - The objective of the risk prioritization scheme is to assist the internal auditor in using limited resources more effectively. Usage involves the interpretation and application of the risk assessment resulting from the utilization of the first three parts of the audit risk prioritizing scheme.

Part 1 - Identification of the Risk Dimensions

The importance of having risk dimensions is to categorize audit risk by the determinant for that risk. This is important because the audit risk characteristics within a dimension or determinant are more closely related than the characteristics between dimensions. This concept can be helpful in both managing audit risk from the data processing perspective, and selecting specific characteristics to investigate from an audit perspective.

Part 2 - Identification of Audit Risk Characteristics

Risk characteristics are attributes of automated information systems which correlate to operational behavior of the automated information system. The presence or absence of these system attributes can be used to predict behavior. An analogy would be predicting the probability of a heart attack by using an individual's heart attack risk characteristics such as blood pressure, weight, family health history, and amount of cigarettes smoked.

The presence or absence of these characteristics can be used to predict whether a specific person might have a heart attack (i.e., a specific human behavior). While the word risk is used, it is not meant to imply that the undesirable event will occur but, rather, that the probability of some type of behavior (e.g., a heart attack) can be predicted. A prioritizing scheme will tell how probable the heart attack is.

The proposed "straw man" characteristics recommended for evaluating each of the three audit risk dimensions are presented in Figure B.1. This straw man risk model is designed to identify and explain the characteristics associated with the three audit risk dimensions. These are the characteristics that most commonly appear in audit risk models currently used by auditors, and are believed to be those which can help auditors predict the operational performance of information systems for audit purposes. Figure B.1 has been placed at the end of this paper so that the attendees may detach it for use in their discussions.

Part 3 - Analysis of the Audit Risk Characteristics

This part of the audit risk prioritizing scheme is designed to measure the degree of audit risk associated with each individual characteristic. The objective of this measurement is twofold. First is to determine the degree of importance of each characteristic in representing the magnitude of audit risk/exposure (i.e., weighting of characteristics among the population of characteristics) and second, to determine the applicability of that characteristic to the specific automated information system being assessed (to determine whether the characteristic is present or absent in a manner that could cause an unfavorable event to occur; for example, if an individual was overweight it would be indicative of a possible undesirable event such as a heart attack).

There are five approaches used to measure the applicability of a characteristic to predict a favorable or unfavorable result. These are:

1) Relational considerations - This asks the auditor to divide the application systems into three risk categories, e.g., high, medium, and low, and then determine into which category the system being assessed falls. For example, an NBS study[1] has shown that the larger the size of a computer program, the more difficult it is to implement. From a relational perspective, the auditor decides whether the size of the program for the system being assessed will fall within the largest third sizewise for the department, the middle third sizewise, or the lowest third sizewise. The largest third would be considered to have the highest risk.

[1] NBS Special Publication 500-99 entitled "Structured Testing: A Software Testing Methodology Using the Cyclomatic Complexity Metric," issued December 1982.

2) Factors relating to risk - This approach attempts to relate specific factors to the expected outcome. The auditor need only determine which factors are applicable to the system under assessment to determine the degree of audit risk. For example, in assessing a data validation characteristic, a factor relating to low risk would be extensive data validation including range, alphabetic, check digit, and relationship tests; while high-risk systems might be those that only use alphanumeric tests.

3) Dollar risk - Using the annual loss expectancy formula (i.e., frequency of occurrence times loss per occurrence) the dollar value associated with each characteristic can be used to determine the magnitude of risk for that characteristic.

4) Audit analysis - This method requires the auditor to conduct sufficient study to determine the potential vulnerability. The most common approach to doing this is an assessment of the system of internal controls in order to identify vulnerabilities associated with the characteristic in question. Again, if the characteristic was data validation, the audit review could determine the effectiveness of the data validation controls to reduce the specific audit risks reducible by data validation controls.

5) Statistical regression analysis- Over a period of time the audit group can record system characteristics and actual operational behavior. Feeding that information into statistical regression analysis, the auditor can determine specific correlation between the various attributes of the characteristics compared to the actual operational behavior of the information system. While this is the statistically proper approach, it can also be very time-consuming and costly to obtain.

Experiences of audit risk model users indicate that the two most popular approaches are relational risk (i.e., high, medium, and low) and risk factors to determine the applicability of the characteristics to the system under review.

Part 4 - Use of the Audit Risk Assessment

The audit risk prioritizing scheme can be used by both data processing and audit personnel. Data processing personnel can use the risk scheme to identify the attributes that may cause the system to be unsuccessful and manage those risks by changing developmental approaches.

The performance of the first three parts of the audit risk scheme will result in the identification of the audit risk characteristics applicable to the automated information system under review, and some indication of the magnitude or degree of applicability. This audit risk information can then be used by internal auditors in any or all of the following manners:

1) Audit risk score - This usage allocates points in accordance with the magnitude of risk associated with each characteristic. The most common scoring method is to divide the risk characteristic into specific subcategories as was illustrated earlier in the data validation example. If the application being assessed falls into the high-risk category, it would be assigned three points, medium risk, two points, and low risk, one point. If a more sophisticated scoring method is wanted, the individual characteristics can be weighted. For example, one characteristic can be considered to be twice as important as another, and thus is multiplied by the weight 2 to give an individual characteristic risk score. The resulting risk score is normally compared to other scores developed for the same department. Thus, risk scoring is normally used to determine relative risk between applications, and the score is not used to determine an absolute measure of risk, such as temperature of the human body, which has an absolute meaning.

2) Create an audit risk profile - An audit risk profile is a pictorial representation of the various risk characteristics measured. While the audit risk score shows audit risk for the entire automated information system, the risk profile shows the relational risk among the various risk characteristics. The objective of the risk profile is to graphically illustrate what characteristics contribute to the total audit risk, and in what proportion.

3) Modification of the characteristics contributing to audit risk - Both the auditor and systems analyst can use the audit risk scheme to identify those characteristics which may cause the information system to be less successful than proposed. For example, if the application project personnel do not understand the computer technology being used, the probability of success of the information system being developed diminishes. Once the characteristics that may cause the system to be less successful than desired are known, those characteristics can be altered such that the probability of the system being successful increases. In our example where the project personnel do not understand the proposed technology, a technology which the project group does know can be substituted and the probability of success will increase.

4) Allocation of audit resources - The information gathered during the audit risk analysis can be used as a basis for allocating audit resources to review application systems and/or review specific aspects of those systems. For example, high-risk information

systems may receive extensive reviews, medium risk, cursory reviews, and low risk, no reviews. For those systems reviewed, the area of review can be selected based on the high-risk characteristics. For example, if computer technology is a high-risk characteristic, the auditors may want to expend time reviewing how effectively the project team is using that technology.

5) Data base of risk characteristics - The information gathered during this process should be saved and used for two purposes. The first use is to improve the audit risk prioritization scheme to make it more predictive of audit risk; and the second use is to assist data processing management in structuring and planning projects such that those projects will have the highest probability of success.

REFERENCES USED TO BUILD THE "STRAW MAN"AUDIT RISK PRIORITIZING SCHEME

The major references used in creating this "straw man" prioritizing scheme were:

1) OMB Circular A-123, "Internal Control Systems," August 16, 1983.

2) U.S. General Accounting Office document on internal control-- "Evaluating Internal Controls in Computer-Based Systems - Audit Guide" June 1981

3) Computer Control and Audit by William Mair, Keagle Davis, and Donald Wood, published by The Institute of Internal Auditors (1977)

4) ESTIMACS software package marketed by Management and Computer Services, Valley Forge, PA

5) PANRISK audit software package and manual, originally marketed by Pansophic Systems, Oak Brook, IL and now called IST/RAMP and marketed by International Security Technology, Inc. of New York City, its originator.

6) "Portfolio Approach to Information Systems" by F. Warren McFarlan, Harvard Business Review, September-October 1981

7) FIPS PUB 65, "Guideline for Automatic Data Processing Risk Analysis" August 1, 1979

8) U.S. General Accounting Office "Standards for Internal Controls in the Federal Government", 1983

FIGURE B.1

RISK DIMENSION CHARACTERISTICS

CHARACTERISTICS FOR THE RISK DIMENSION -- PROJECT SIZE

1. Size of user area - Number of employees, size of user budget, number of user functions.

2. Data processing breadth - Size of project as expressed in number of project staff, size of project budget, or number of man-months to produce.

3. Size of information system - Expressed in number of programs, size of programs, number of transactions.

4. Expected frequency of change - The number and/or size of changes that will be made to the initial needs statement.

5. Number of unique logical business inputs that the system will process - Expressed in number of business transactions processed in the course of a day.

6. Number of unique logical business outputs generated by the system - Number of business transactions or reports or messages produced per day by the system.

7. Number of logical files (views) that the system will access - The number of individual files or data base subschemas that will be accessed by the system during the totality of system processing.

8. Number of major types of on-line inquiry expected - The number of requests that will be made by users other than the normal business outputs generated by the information system.

9. Telecommunications - The use of communication facilities in conjunction with automated information systems. Risk associated with the number of terminals, amount of hard-copy documents produced, and the sophistication of processing.

FIGURE B.1 (continued)

CHARACTERISTICS FOR THE RISK DIMENSION -- EXPERIENCE WITH TECHNOLOGY

1. Makeup of project team in relationship to technology used - The inclusion on the project team of the necessary skills to effectively utilize the information system technology, e.g.,the inclusion of data base personnel for data base-related projects.

2. Applicability of the data processing design methodologies and standards to the technology in use - The adaptability of the existing data processing methodologies and standards to the technology being used. For example, if the information system is being developed under prototyping, are the design methodologies and standards applicable to prototyping?

3. Margin of error - The amount of time between the entry of a business transaction and the response to that transaction. For example, is there reasonable time to make adjustments, corrections, or perform analyses before the transaction is completed?

4. Technical complexity of the information system - The number of tasks and interrelationship between those tasks that must be accomplished to satisfy the user needs.

5. Adaptability to change - The ease with which it is expected that changes to the information system requirements can be incorporated into the information system. This will be dependent upon the architecture of the system and its adaptability to the user information needs.

6. Utilization of equipment - How much the information system will push the equipment to its capacity to meet user needs. For example, if a two-second response is needed and given the complexity of the tasks and the volume of work, what is the amount of tolerance within the system capacity to meet those processing needs?

7. Personnel - Skill level, number, and knowledge of user processing of the project team members including any supporting technical staff(s).

FIGURE B.1 - (continued)

8. Documentation - Amount, currentness, type, and usability of the documents supporting the automatic information system.

9. Pioneering aspects - The newness of the technology and/or technological approaches used in this application system. The newness can be either within the organization (i.e., the first time any project has used this technology, such as data base technology) or the newness of the technology as offered by the vendors.

1Ø. How knowledgeable is the user in data processing technology - Determines whether the user personnel can understand the implications of use of data processing technology, and their ability to define requirements and discuss requirements in relationship to its impact on technology.

11. Data processing knowledge of user tasks - The ability of data processing personnel to challenge the accuracy and need of user requirements in relationship to the mission and tasks performed by the user.

12. Degree of complexity of processing logic - Measures whether the logic needed to perform the user requirements will be simple, average, or complex.

13. Need for automated error detection and correction procedures - Measures the complexity of the procedures that need to be incorporated into the information system to detect inaccurate or incomplete input transactions and make automatic correction to those errors.

FIGURE B.1 - (continued)

CHARACTERISTICS FOR THE RISK DIMENSION -- PROJECT STRUCTURE

1. Organizational breadth - The number of diverse organizational units involved in the application system and/or the number of user organizations that must sign off on the requirements definition.

2. Political implications of implementing the information system - The level of agreement among all units in the organization as to the need for the system and the approach being used to accomplish the system objectives.

3. Specificity of user requirements - The level of detail in which the requirements are specified. Measures the amount of additional detail and/or decisions that need to be made before programs can be coded.

4. Problems associated with current system performance - Measures the amount of problems that are occurring in the current system as implemented. The thesis is that performance problems in current systems may not be correctable by a new system.

5. Availability of backup hard-copy documents - The number of original source documents and hard-copy format that will be produced and retained during system processing.

6. Level of user management agreement on system objectives - The agreement within the user(s) department on the stated objectives for the system.

7. Percentage of the proposed information system that is already performed by the user - Measures the newness of the information system tasks to the user area. Differentiates between existing tasks being automated, and new tasks (new meaning a new method for processing).

FIGURE B.1 - (continued)

8. Importance/criticality of the business system to the user - Measures the importance of this specific information system to the user as it relates to the user completing the mission of the user function.

9. Project management approach and structure - The organization of the project in relationship to the size of the project and the technology being utilized. Includes such consideration as division of duties within the project, relationship between the user and data processing personnel, as well as the management and status reporting structures.

APPENDIX C

PCIE/NBS INVITATIONAL WORKSHOP

CO-CHAIRPERSONS: Bonnie T. Fisher & Zella G. Ruthberg

DISCUSSION GROUPS MEMBERSHIP

GROUP A

John Lainhart (Group Leader)	Department of Transportation Office of Inspector General Director, Office of ADP Audits and Technical Support
Robert L. Gignilliat (Recorder)	Department of Health and Human Services Senior Systems Security Officer
Nander Brown	Federal Home Loan Mortgage Corporation Assistant General Auditor
Peter S. Browne	Profile Analysis Corporation President
James E. Haines	Boeing Computer Services Co. Director, Quality Assurance
Kenneth Jannsen	Blue Cross/Blue Shield of Illinois Director, Internal Audits
Jarlath O'Neill-Dunne	Coopers and Lybrand, (New York, NY) Partner
Tyrone Taylor	National Aeronautics and Space Administration, Space Station Management Analyst
John Van Borssum	Security Pacific National Bank Vice President, EDP Auditor
J. Armand Villemaire	Department of Defense Air Force Audit Agency Staff Auditor
Patricia D. Williams	Department of Treasury Internal Revenue Service Head of Security

GROUP B

Barry R. Snyder (Group Leader)	General Accounting Office, IMTEC Group Director, Technical Services
Mark J. Gillen (Recorder)	Department of Treasury Internal Revenue Service Internal Audit Manager
Robert P. Abbott	EDP Audit Controls, Inc. President
Lorretta Ansbro	Federal Reserve Bank of New York Audit Official
Stephen F. Barnett	Department of Defense Computer Security Center Chief, Office of Application System Evaluation
Larry Bergman	Boeing Computer Services Co. EDP Audit Manager
Robert Berndt	Bank of America (San Francisco) Vice President, EDP Audit Manager
Keagle Davis	Touche Ross & Co. (Jacksonville) Partner
Michael Goldfine	General Motors Corporation Assistant Director, Audit Staff
Ralph E. Gooch	Department of Treasury Financial Management Services Chief of Security Branch
Michael G. Houston	Department of Defense Office of Inspector General Program Director, Audit Policy and Oversight
Jack Wheeler	General Accounting Office, IMTEC Special Assistant, Technical Services

GROUP C

Wallace O. Keene (Group Leader)	Department of Health & Human Services Acting Deputy Assistant Secretary for Management Analysis and Systems
Allen Winokur (Recorder)	Navy Audit Service EDP Auditor
David L. Decker	Department of Housing and Urban Development Office of Inspector General Director, EDP Audit
Frederick Gallegos	General Accounting Office (Los Angeles) Manager, Management Services Group
Carole A. Langelier	DeLoitte, Haskins and Sells (Washington, D.C.) Partner
Joseph T. McDermott	Department of Defense Office of Inspector General/AUDIT Program Manager
Gerald Meyers	EDP Audit Consultants Managing Partner
Carl A. Pabst	Touche Ross & Company (Los Angeles) Partner, Director of EDP Audit
Frederick G. Tompkins	ORI, Incorporated Senior Principal Scientist
Hart J. Will, Ph.D.	University of Victoria, B.C. Professor of Public Administration

GROUP D

Larry Martin (Group Leader)	Department of Energy Manager, Computer Security Program
Gail L. Shelton (Recorder)	Department of Health & Human Services Office of Inspector General Program Analyst
James Cox	Department of Health & Human Services Office of Inspector General EDP Auditor
Tim Grance, 2nd Lt.	U.S. Air Force Computer Security Program Office Computer Security Staff Officer
Michael J. Henitz	Peat Marwick Mitchell & Co. Computer Audit Office Partner
William M. Hufford	Sun Banks, Inc. Vice President, EDP Audit Manager; EDP Auditors Association Regional President
Stanley Jarocki	Bankers Trust of New York Vice President, Group Manager
William C. Mair	Touche Ross & Co. (Detroit) Partner
Thomas Nugent	Department of Navy, NARDAC Computer Specialist
Kenneth A. Pollock	EDP Auditors Foundation Director of Research
F. A. Schlegel	Management and Computer Services, Inc. President
D. L. Von Kleeck	Management and Computer Services, Inc. General Manager
H. C. Warner	Florida Power Director, Internal Audits

GROUP E

Douglas B. Hunt (Group Leader)	National Aeronautics and Space Administration Office of Inspector General Director, Technical Services
William C. Lee (Recorder)	Department of Commerce Office of Inspector General Office of Automated Information Systems Computer Specialist
Philip Carollo	Sears, Roebuck and Company Director, EDP Audits
Don Colner	Basic Data Systems, Inc. President
Robert V. Jacobson	International Security Technology, Inc. President
Thomas Lux	Touche Ross & Company (Chicago) Audit Supervisor
Jim Manara	Security Pacific National Bank Quality Assurance Division Vice President
Brian McAndrew	U.S. Navy Navy Audit Service Assistant Director, Audit Policy
Brian Morse	Coopers & Lybrand (Washington, D.C.) Partner
Benson J. Simon	Environmental Protection Agency Program Analyst
Jane Tebbutt	Department of Health and Human Services Office of Inspector General Director, Interagency Projects Division

APPENDIX D

TWO RISK SCORING METHODS

D.1 A Simple Scoring Approach

D.1.1 The Scoring Method

This method risk scores each system by using Figure D.1 to calculate the scores as described below.

Step 1 - Assign Importance Weights. A weight, reflecting the importance of the dimension to the system under review, is assigned to each of the five dimensions shown in Figure D.1. This weight will in turn reflect the importance of the dimension's characteristics to the system under review. One of the two suggested weighting schemes[1] shown in Figure D.1 can be used, although specific situations may require modification of these. The weights in set 1 add up to an arbitrary number while those in set 2 add up to 1ØØ. Set 2 allows for easy conversion of the weights to percentages.

Step 2 - Assign Risk Level. For each dimension assign a risk level from 1 - 5 which reflects the degree of risk for that dimension. Suggested risk level values are:

5 = High Risk
3 = Medium Risk
1 = Low Risk

For example, a system with demonstrated reliability would pose a low risk and warrant a low risk level value (=1).

Step 3 - Calculate Dimension Risk Score. The dimension risk score is its weight times its risk level.

Step 4 - Calculate System Risk Score. For a Level I type system risk score, use the risk score for the Criticality/Mission Impact dimension. The Level II system risk score is the sum over each of the five dimension's risk score.

Step 5 - Rank System Scores. Perform Steps 2, 3, and 4 for each system under consideration and rank systems numerically from high to low. The highest scoring systems pose the highest risk and therefore deserve more audit/review attention.

D.1.2 Example of a Scored System

Table D.1 is an example of a calculated risk score for one

[1] The suggested weights were derived from data collected from representatives attending the PCIE Workshop.

Figure D.1 SYSTEM RISK SCORING - SIMPLIFIED METHOD

SYSTEM ____________________

Dimensions	Weight		Risk Level	Weighted Score	Comments
	1.	2.			
1. Criticality/Mission Impact	(30)	(50)			
2. Size/Scale/Complexity	(15)	(15)			
3.Environment/Stability	(10)	(10)			
4. Reliability/Integrity	(10)	(10)			
5. Technology Integration	(10)	(15)			
			System Score		

Table D.1 SYSTEM RISK SCORING - SIMPLIFIED METHOD EXAMPLE

SYSTEM Research Grants System

Dimensions	Weight 1.	Weight 2.	Risk Level	Weighted Score	Comments
1. Criticality/Mission Impact	30 (20)	(50)	5	150	Grants are major function; but manual operation is possible.
2. Size/Scale/Complexity	15 (15)	(15)	3	45	Size is small compared to all others.
3.Environment/Stability	10 (10)	(10)	3	30	It is a stand-alone system with known responsibilities and requirements.
4. Reliability/Integrity	10 (10)	(10)	5	50	There have been numerous instances of fraud in the present system.
5. Technology Integration	15 (10)	(15)	5	75	Will use the first data base package and a new communication method.
			System Score	350	

system. The suggested weights of set 1 in Figure D.1 were used except for Technology Integration. This was given a higher weight of 15 because, in the organization, almost all new systems have failed whenever any new technology is introduced. The five dimensions were then given a risk level value based on audit knowledge and surveys. A total score of 350 was then calculated for ranking purposes.

D.2 A Detailed Scoring Approach

D.2.1 Risk Scoring a Dimension

Although the "strawman" paper describes five approaches to analyzing risk (See Appendix B), a method of ranking and rating is suggested here as an approach commensurate with the softness of the data available. Each dimension of the scheme is rated and ranked separately, with scores then combined. Since Criticality/ Mission Impact is the Level I dimension of the proposed scheme, one would analyze this dimension first. The procedure is as follows:

First, the n characteristics <u>within a dimension</u> are ranked according to their respective importance to that dimension. The importance rank number of characteristic i is I(i) and ranges from 1 to n with n correlated with the most important characteristic. For operational systems one can use discriminant analysis applied to equal sets of known system failures and successes to obtain this ranking. For developmental systems a consensus view of audit management can be used, ideally obtaining sponsor/user input.

Second, the importance ranking number, I(i), is converted to an importance weighting factor, W(i), that is normalized to 20. (The reason for selecting 20 will be explained in Section D.2.3.) This means that the sum of the weighting factors for the characteristics within a dimension is set to 20 (or normalized to 20). Since each of the five dimensions has a different number of characteristics and we wish to treat the dimensions as equals, normalization will guarantee that the risk score range for each dimension will be the same.

The normalization factor, F, is the number which converts the importance ranking number I(i) to the importance weighting factor W(i). The relationships are:

$$(1)\quad W(i) = F \times I(i)$$

$$(2)\quad \sum_{i=1 \text{ to } n} W(i) = \sum_{i=1 \text{ to } n} F \times I(i) = 20$$

Solving equation (2) for F, we find

$$(3)\ F = \frac{20}{\sum_{i=1 \text{ to } n} I\ (i)}$$

and substituting for F in equation (1) yields the importance weighting factor W(i) for characteristic i, i.e.,

$$(4)\quad W\ (i) = 20 \times \frac{I\ (i)}{\sum_{i=1 \text{ to } n} I\ (i)}$$

Third, each characteristic is rated with respect to the risk of occurrence. One of the following risk ratings, R(i), is assigned to characteristic i.

R (i) = 3 (for High Risk)

R (i) = 2 (for Medium Risk)

R (i) = 1 (for Low Risk)

These ratings can be assigned by the auditor, again with user assistance if appropriate.

Finally, a Risk Score for that dimension is obtained by multiplying the importance weighting by the risk rating of the characteristic and summing over the characteristics for that dimension. The equation for this is the following:

$$DRS\ (j) = \sum_{i=1 \text{ to } n} W\ (i) \times R\ (i)$$

where i = characteristics 1 to n

W (i) = importance weighting for characteristic i
R (i) = risk rating for characteristic i

DRS (j) = dimension j's risk score, j = 1 to 5

The Risk Score for each of the five dimensions will range from 20 to 60 using these importance weighting and risk rating number assignments.

D.2.2 Level I System Risk Score

After completing a Level I review for an organization's universe of AISs, using the analysis scheme in Section D.2.1, one can use the Criticality/Mission Impact dimension risk score as a first order approximation to a system risk score. Since these risk scores have all been normalized to the same number (2Ø), it is possible to compare these risk scores across AISs and eliminate from further consideration AIS's having a low risk with respect to Criticality/Mission Impact.

D.2.3 Level II Review Considerations

If it is decided that the more detailed Level II review is appropriate and/or affordable, one must decide upon a sequence for reviewing the remaining dimensions of the high risk critical AISs. While there is <u>no "correct" way</u> to do this, it might be appropriate to consider the following.

Since the Environment/Stability dimension includes the organization's general controls, including the strength and involvement of quality assurance, project management, and security functions throughout the SDLC (of both systems and major enhancements to existing systems), it may be most useful to review this dimension first in a Level II review. These general controls would heavily impact the need for audit coverage as well as the scope and expertise necessary in that coverage. The EDP auditors could confidently reduce their scope and related testing of applications if they could rely on the organization's general controls and the safeguards these various review functions provide in the SDLC process. Any ranking or prioritizing of the elements in the work priority scheme, beyond the overriding factors described above (i.e., external influence and mission criticality), could <u>not</u> be reasonably accomplished without a survey of the organization's general and applications controls and/or without an institutional knowledge of the organization, its SDLC process, and any facts and circumstances affecting system development activities. The characteristics in all four Level II dimensions should be weighted and rated in the light of such background information, and the dimension risk score, DRS, obtained for each of the four Level II dimensions.

D.2.4 Level II System Risk Score

As a second order approximation one can treat the dimensions as equal contributors to the risk score for the AIS as a whole. Under this assumption the system risk score, SRS, is then a simple sum of the five dimension risk scores, DRS.

$$(5) \quad SRS = \sum_{j=1 \text{ to } 5} DRS\ (j)$$

where SRS = system risk score

j = dimensions 1 to 5

DRS (j) =dimension j's risk score

Since DRS(j) can range from 2Ø to 6Ø, SRS will range from 1ØØ to 3ØØ. The choice of 2Ø for the sum of the weights of the characteristics within a dimension is arbitrary and was made in order to place SRS in a reasonable range for comparing one system's risk score to another's.

D.2.5 An Example

It may be a useful exercise to go through an example of the arithmetic involved. Assume we wish to calculate dimension risk scores and system risk scores for two AISs. To simplify matters we shall assume small numbers of characteristics for each dimension. Dimension 1 has four characteristics, dimension 2 has three characteristics, dimension 3 has five characteristics, dimension 4 has three characteristics and dimension five has 2 characteristics. The importance rankings I(i) and the risk ratings R(i) are obtained from audit management and the auditor respectively. The rest of the numbers in Tables D.2 and D.3 are calculated using equations (1) - (5). (A practice template of the table has been included in Figure D.2 to assist the reader in learning the methodology.)

Using dimension 1 as a first order system risk score, we find AIS 1, with DRS = 42, is more at risk than AIS 2, with DRS = 38. We obtain the second order risk score by adding the five dimension risk scores for each AIS. Using these numbers, AIS 1, with SRS = 191.4, is again more at risk than AIS 2, with its SRS = 18Ø.Ø. Only experience with the method will enable the reviewer to obtain more refined interpretations of the calculations.

Figure D.2 PRACTICE TEMPLATE FOR RISK SCORING OF AN AIS

AIS ______

DIMENSION	I(i)	F	W(i)	R(i)	W x R	DRS(j)

DIM 1
C(1)
C(2)
C(3)
C(4)						

DIM 2
C(1)
C(2)
C(3)						

DIM 3
C(1)
C(2)
C(3)
C(4)
C(5)						

DIM 4
C(1)
C(2)
C(3)						

DIM 5
C(1)
C(2)						

					SRS	

Table D.2 DIMENSION RISK SCORES AND SYSTEM RISK SCORES FOR AIS 1

AIS 1

DIMENSION	I(i)	F	W(i)	R(i)	W x R	DRS(j)
DIM 1						
C(1)	2	2	4	1	4	
C(2)	1	2	2	2	4	
C(3)	4	2	8	2	16	
C(4)	3	2	6	3	18	
	10	_	20	_	42	
						42.0
DIM 2						
C(1)	3	10/3	10	1	10	
C(2)	2	10/3	20/3	2	40/3	
C(3)	1	10/3	10/3	3	10	
	6	_	20	_	33.3	
						33.3
DIM 3						
C(1)	4	4/3	16/3	3	16	
C(2)	2	4/3	8/3	2	16/3	
C(3)	5	4/3	20/3	1	20/3	
C(4)	1	4/3	4/3	2	8/3	
C(5)	3	4/3	4	3	12	
	15	_	20	_	42.7	
						42.7
DIM 4						
C(1)	1	10/3	10/3	3	10	
C(2)	3	10/3	10	3	30	
C(3)	2	10/3	20/3	1	46.7	
	6	_	20	_	46.7	
						46.7
DIM 5						
C(1)	1	20/3	20/3	2	40/3	
C(2)	2	20/3	40/3	1	40/3	
	3	_	20	_	26.7	
						26.7
					SRS	191.4

1st Order SRS (Range = 20 to 60) = DRS(1) = 42.0

2nd Order SRS (Range = 100 to 300) = SRS = 191.4

TABLE D.3 DIMENSION RISK SCORES AND SYSTEM RISK SCORES FOR AIS 2

AIS 2

DIMENSION	I(i)	F	W(i)	R(i)	W x R	DRS(j)
DIM 1						
C(1)	4	2	8	3	24	
C(2)	2	2	4	1	4	
C(3)	1	2	2	2	4	
C(4)	3	2	6	1	6	
	10	_	20	_	38	
						38.0
DIM 2						
C(1)	2	10/3	20/3	3	20	
C(2)	1	10/3	10/3	1	10/3	
C(3)	3	10/3	10	2	20	
	6	_	20	_	43.3	
						43.3
DIM 3						
C(1)	5	4/3	20/3	3	20	
C(2)	3	4/3	4	1	4	
C(3)	1	4/3	4/3	2	8/3	
C(4)	2	4/3	8/3	1	8/3	
C(5)	4	4/3	16/3	3	16	
	15	_	20	_	45.4	
						45.4
DIM 4						
C(1)	2	4	20/3	2	40/3	
C(2)	2	4	10	1	10	
C(3)	1	4	10/3	3	10	
	5	_	20	_	33.3	
						33.3
DIM 5						
C(1)	2	20/3	40/3	1	40/3	
C(2)	1	20/3	20/3	1	20/3	
	3	_	20	_	20	
						20.0
					SRS	180.0

1st Order SRS (Range = 20 to 60) = DRS(1) = 38.0

2nd Order SRS (Range = 100 to 300) = SRS = 180.0

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

U.S. DEPT. OF COMM.

BIBLIOGRAPHIC DATA SHEET *(See instructions)*

1. PUBLICATION OR REPORT NO.
NBS IR-86-3386

2. Performing Organ. Report No.

3. Publication Date
JULY 1986

4. TITLE AND SUBTITLE
Work Priority Scheme for EDP Audit and Computer Security Review

5. AUTHOR(S)
Zella G. Ruthberg, and Bonnie T. Fisher

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

National Bureau of Standards
Department of Commerce
Gaithersburg, MD 20899

7. Contract/Grant No.

8. Type of Report & Period Covered

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

National Bureau of Standards
Department of Commerce
Gaithersburg, MD 20899

and

Department of Health & Human Services
Office of Inspector General
330 Independence Avenue, SW
Washington, DC 20201

10. SUPPLEMENTARY NOTES
This report documents a synthesis of ideas developed at an invitational workshop sponsored by the National Bureau of Standards and the Department of Health & Human Services

□ 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 report describes a high level risk analysis for Automated Information Systems (AISs) that can be used by computer security reviewers and EDP auditors to prioritize their non-discretionary and discretionary review activities for these AISs. It divides the risk analysis problem into five areas of risk concern (called dimensions) with each area defined by a set of characteristics. The five dimensions are: Criticality/Mission Impact, Size/Scale/Complexity, Environment/Stability, Reliability/Integrity, and Technology Integration. The report presents a possible two-level scoring scheme which calculates the level of risk for each dimension, uses the Criticality score as a first order system risk score, and then combines all five dimension risk scores for a second order system risk score. An approach for deriving an EDP audit or computer security review plan using these scores is outlined.

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

audit/review plan; automated information system risk analysis; computer security review; criticality/mission impact; discretionary audit/review; EDP audit; environment/stability; non-discretionary audit/review; reliability/integrity; risk score; size/scale/complexity; technology/integration

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
60

15. Price
$11.95