

AD-A246 965



2

NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS

**DE-CERTS: A DECISION SUPPORT SYSTEM
FOR A COMPARATIVE EVALUATION METHOD FOR
RISK MANAGEMENT METHODOLOGIES AND TOOLS**

by

Leonard A. Crump Jr.
and
James G. Pound

September 1991

Thesis Advisor:

Magdi N. Kamel

Approved for public release; distribution is unlimited

92 3 03 250

92-05741



REPORT DOCUMENTATION PAGE			
1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED		1b RESTRICTIVE MARKINGS	
2a SECURITY CLASSIFICATION AUTHORITY		3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.	
2b DECLASSIFICATION/DOWNGRADING SCHEDULE			
4 PERFORMING ORGANIZATION REPORT NUMBER(S)		5 MONITORING ORGANIZATION REPORT NUMBER(S)	
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b OFFICE SYMBOL (If applicable) 55	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School	
6c ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000		7b ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000	
8a NAME OF FUNDING/SPONSORING ORGANIZATION	8b OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8c ADDRESS (City, State, and ZIP Code)		10 SOURCE OF FUNDING NUMBERS	
		Program Element No	Project No
		Task No	Work Unit Accession Number
11 TITLE (Include Security Classification) DE-CERTS: A Decision Support System for a Comparative Evaluation Method for Risk Management Methodologies and Tools			
12 PERSONAL AUTHOR(S) Crump, Leonard A. Jr. and Pound, James G.			
13a TYPE OF REPORT Master's Thesis	13b. TIME COVERED From To	14. DATE OF REPORT (year, month, day) 1991 September	15 PAGE COUNT 154
16 SUPPLEMENTARY NOTATION The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
17 COSATI CODES		18 SUBJECT TERMS (continue on reverse if necessary and identify by block number)	
FIELD	GROUP	SUBGROUP	
		Risk, Risk Management, Risk Assessment, Risk Analysis, Computer Security, Decision Support System	
19 ABSTRACT (continue on reverse if necessary and identify by block number) A new approach was recently proposed to effectively and objectively evaluate risk management methodologies and tools for their suitability to a given organizational situation. The proposed approach, known as CERTS, is based on defining suitability in terms of criteria which in turn are described in terms of attributes and metrics. Using the Analytic Hierarchy Process, this thesis develops the CERTS approach into a Decision Support System, that could be used easily and effectively by organizations for selecting a risk management methodology or tool. The thesis also applies the developed DSS to three case studies to gain insights on the applicability of the DSS.			
20 DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED UNLIMITED <input type="checkbox"/> SAME AS REPORT <input type="checkbox"/> DTIC USERS		21 ABSTRACT SECURITY CLASSIFICATION	
22a NAME OF RESPONSIBLE INDIVIDUAL Magdi N. Kamel		22b TELEPHONE (Include Area code) (408) 646-2494	22c OFFICE SYMBOL AS/KA

Approved for public release; distribution is unlimited.

**DE-CERTS: A DECISION SUPPORT SYSTEM
FOR A COMPARATIVE EVALUATION METHOD FOR
RISK MANAGEMENT METHODOLOGIES AND TOOLS**

by

**Leonard A. Crump Jr.
Major, United States Army
B.S., Fitchburg State College, 1979**

and

**James G. Pound
Lieutenant, Supply Corps, United States Navy
B.A., Aurora College, 1975**

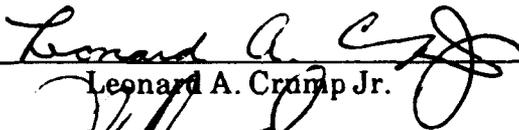
Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

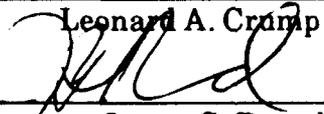
from the

**NAVAL POSTGRADUATE SCHOOL
September 1991**

Authors:

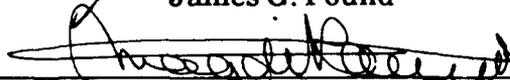


Leonard A. Crump Jr.



James G. Pound

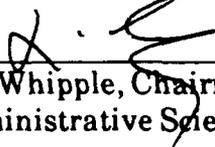
Approved by:



Magdi N. Kamel, Thesis Advisor



Lance J. Hoffman, Second Reader



Professor David R. Whipple, Chairman
Department of Administrative Sciences

ABSTRACT

A new approach was recently proposed to effectively and objectively evaluate risk management methodologies and tools for their suitability to a given organizational situation. The proposed approach, known as CERTS, is based on defining suitability in terms of criteria which in turn are described in terms of attributes and metrics. Using the Analytic Hierarchy Process, this thesis develops the CERTS approach into a Decision Support System, that could be used easily and effectively by organizations for selecting a risk management methodology or tool. The thesis also applies the developed DSS to three case studies to gain insights on the applicability of the DSS.



Accession For	
NTIS GRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

TABLE OF CONTENTS

I. INTRODUCTION 1

 A. BACKGROUND 1

 B. OBJECTIVE 2

 C. RESEARCH QUESTION 3

 D. SCOPE, LIMITATIONS AND ASSUMPTIONS 3

 E. RESEARCH METHODOLOGY 4

 1. Literature Review 4

 2. Implementing the Comparative Method 5

 3. Testing the Proposed Method 6

 F. ORGANIZATION OF STUDY 6

II. CERTS: A COMPARATIVE EVALUATION METHOD FOR RISK
MANAGEMENT METHODOLOGIES AND TOOLS 7

 A. INTRODUCTION 7

 B. THE CERTS APPROACH 8

 1. A Measure for Suitability 9

 2. Steps for Suitability 10

 C. CRITERIA, ATTRIBUTES, AND METRICS 11

 1. Application of the Metrics 13

 2. Performance of the Metrics 13

 D. CONCLUSION 14

III.	THE ANALYTIC HIERARCHY PROCESS	15
A.	INTRODUCTION	15
B.	THE AHP PROCESS	16
C.	CONCLUSION	25
IV.	IMPLEMENTATION OF CERTS USING THE ANALYTIC HIERARCHY PROCESS	26
A.	INTRODUCTION	26
B.	IMPLEMENTATION OF CERTS USING AHP	27
1.	Consistency	29
2.	User Interface	29
3.	Adaptability	30
4.	Feasibility	30
5.	Completeness	31
6.	Validity	31
7.	Credibility	32
C.	INCORPORATING ALTERNATIVES TO THE HIERARCHY	32
1.	Alternative Risk Management Packages	32
2.	Assigning Weights to the Alternatives	33
V.	APPLICATION OF THE DSS TO CASE STUDIES	36
A.	INTRODUCTION	36
1.	Application of CERTS DSS	36
2.	Disclaimer for Case Scenarios	37
B.	CASE SCENARIO DESCRIPTIONS	38

1. Case Scenario One: Distributed Wide Area	
Network (WAN)	38
a. Physical Environment	38
b. Equipment	39
c. Personnel	39
d. Data Environment	40
e. Operating Systems	41
f. Management Philosophy and Concerns . . .	43
2. Case Scenario Two: Under Development System -	
Biomed	49
a. Physical Environment	49
b. Equipment	50
c. Personnel	50
d. Data Environment	51
e. Operating Systems	51
f. Administration	51
g. Management Philosophy and Concerns . . .	53
3. Case Scenario Three: Data Center	59
a. Physical Environment	59
b. Equipment	61
c. Personnel	61
d. Data Environment	62
e. Operating Systems	63
f. Administration	64
g. Management Philosophy and Concerns . . .	65

VI.	CONCLUSIONS AND RECOMMENDATIONS	72
A.	CONCLUSIONS	72
1.	CERTS Decision Support System	72
2.	Case Studies	73
B.	RECOMMENDATIONS	74
APPENDIX A.	SUBSUBCRITERIA OF THE DECISION SUPPORT SYSTEM	76
APPENDIX B.	CERTS DSS HIERARCHY	83
APPENDIX C.	DECISION SUPPORT SYSTEM ASSIGNED WEIGHTS FOR ALTERNATIVES	91
APPENDIX D.	CERTS DSS RESULTS FOR WIDE AREA NETWORK CASE STUDY	130
APPENDIX E.	CERTS DSS RESULTS FOR BIOMED CASE STUDY	134
APPENDIX F.	CERTS DSS RESULTS FOR DATA CENTER CASE STUDY	138
LIST OF REFERENCES	142
INITIAL DISTRIBUTION LIST	145

ACKNOWLEDGEMENTS

The authors are extremely grateful for the financial assistance and expertise on risk management packages provided by Irene Gilbert and Nicki Lynch of the National Institute of Standards and Technologies.

Our sincerest gratitude to Professor Magdi Kamel for his guidance, without which this study could not have been completed. He has been an integral part of our thesis process, providing untold support and advice, and keeping us headed in the right direction. Professosr Lance Hoffman provided us with a better perspective. His ability to work and respond so quickly is deeply appreciated.

Last but not least, we want to thank our wives, Jayne Crump and Wanda Pound, who provided support and patience during this extensive effort. An extra special thanks goes to Wanda, who spent numerous hours typing and formatting the thesis. Without her effort, we would still be working on the project.

I. INTRODUCTION

A. BACKGROUND

The need for acceptable computer security risk management practices is becoming more evident throughout the federal and commercial environment because of the sophistication and complexity of today's technology and the increased value society has placed on information. Research over the last four to five years has focused on establishment and refinement of a formalized framework for risk management (Katzke, 1988 and Mayerfeld, 1989), and many automated tools have been developed by commercial and governmental organizations. Despite the attention given to the development of a framework, little has been done to establish a technique for determining which risk management methodology or tool is most suitable for a given organizational situation.

To overcome this deficiency, a new method was recently proposed to effectively and objectively evaluate risk management methodologies and tools for their suitability to a given organizational situation (Garrabrants, Ellis, Hoffman, and Kamel, 1990). The proposed approach, known as CERTS, is based on defining suitability in terms of criteria which in turn are described in terms of attributes. These attributes are further decomposed into metrics that could objectively be

applied to the methodology or tool under consideration for a given organizational situation. A mathematical model could then be used to combine metric evaluations with weights assigned to criteria, attributes and metrics to obtain an overall suitability index of each alternative methodology or tool.

By using the proposed methodology, determining the suitability of particular method or tool becomes standardized, flexible, and expandable. The method is standardized since a uniform set of criteria, attributes, and metrics are used. The method is also flexible because different weights could be assigned to metrics, attributes, and criteria according to the organizational situation. Finally, as the definition of suitability is refined, the method is expandable by simply adding additional metrics, attributes, and criteria.

B. OBJECTIVE

The objective of this research is to develop the CERTS method into a Decision Support System (DSS) that could be used easily and effectively by management personnel for selecting a risk management methodology or tool. Currently the proposed method relies on a series of manual questionnaires which are tedious and time consuming.

In addition to building a Decision Support System the research aims at applying the proposed method. To accomplish this goal, we apply the developed DSS to three hypothetical

case studies. Each case study represents a different environment that requires the use of a risk management tool to assess the risks that each environment faces.

Based on the application of the method to the case studies, we expect to gain useful insight that could be used later to refine the method, by adding, removing, or modifying criteria, attributes or metrics, to accurately select the most appropriate methodology or tool to fit the particular organizational requirement.

C. RESEARCH QUESTION

The main research question addressed by this thesis is: Can an effective Decision Support System based on the CERTS approach be developed to assist organizations in selecting the most appropriate risk management tool for their environment?

A secondary research question is to determine whether the developed decision support system could be applied successfully in different environments to select the best risk management tool.

D. SCOPE, LIMITATIONS AND ASSUMPTIONS

For the purpose of this study, the decision support system was limited to three risk management packages. The three packages selected for inclusion in this study were based upon recommendations by the National Institute of Standards and Technology (NIST) Risk Management Laboratory.

The case studies developed in Chapter V are hypothetical situations developed from cases used by NIST for testing and evaluating the risk management packages at the laboratory. These situations have been expounded upon by the authors to actually test the CERTS Decision Support System.

To allow for testing, comparisons, and familiarization of the risk management packages, the authors spent three days at the NIST Risk Management Laboratory in Gaithersburg, Maryland. Nicki Lynch and Irene Gilbert were invaluable in helping the authors evaluate the three selected packages.

E. RESEARCH METHODOLOGY

To accomplish our objective, the methodology consists of three phases: 1) Literature Review, 2) Implementing the Comparative Method, and 3) Testing the Proposed Method by applying it to three case studies. These phases are detailed below.

1. Literature Review

First, Garrabrants and Ellis' thesis (Garrabrants and Ellis, 1990) was reviewed for background information on CERTS. Second, Thomas Saaty's Analytical Hierarchy Process (Saaty, 1980) was examined. Three candidate risk management tools were selected, tested, analyzed, and compared at the National Institute of Standards and Technologies Risk Management Laboratory for inclusion in the developed DSS.

2. Implementing the Comparative Method

We have found the Expert Choice software to be an excellent vehicle for implementing the proposed technique into a Decision Support System. Expert Choice implements the Analytic Hierarchy Process (AHP), an approach to multi-criteria decision making problems (Saaty, 1982). Under this approach, a decision problem is structured in the form of a hierarchy (tree). The root of the tree is the goal. Intermediate levels of the tree represent the criteria used to accomplish the goal, and at the bottom of the tree are the leaves which represent the alternative choices. Users make comparative judgements in order to establish the relative importance between criteria and the preference of the alternatives with respect to the specific qualities of a criterion.

CERTS fits nicely within the framework of AHP. Concepts of criteria, attributes, and metrics could be incorporated readily at the intermediate levels of an AHP decision hierarchy. At the bottom of the tree would be the candidate methodologies or tools under consideration. Since the proposed metrics are boolean questions, they need to be modified and expressed in a form that allows the assignment of numeric rather than boolean values.

The proposed Decision Support System served as the structure for integrating the suggested modifications to the boolean questions. The system assigned numeric weights to the

modified CERTS method for each methodology or tool. This process completed the development of the CERTS Decision Support System.

3. Testing the Proposed Method

In this phase, the developed Decision Support System is tested by applying it to three case studies. The case studies were developed via input from NIST and the authors. Information inferred from the case studies was applied to the prototype Decision Support System to make a recommended selection for each case situation.

F. ORGANIZATION OF STUDY

Chapter II reviews the CERTS approach. Chapter III explains the underlying premise of the Analytic Hierarchy Process used as the vehicle for implementing the decision support system. Chapter IV describes the implementation of the CERTS Decision Support System. Chapter V details the application of the decision support system to three case scenarios and discusses the results of the DSS for each case. Chapter VI gives conclusions and recommendations about the research and indicates directions for further research.

II. CERTS: A COMPARATIVE EVALUATION METHOD FOR RISK MANAGEMENT METHODOLOGIES AND TOOLS

A. INTRODUCTION

This chapter is designed to assist the reader in understanding the basics of the Comparative Evaluation Method for Risk Management Methodologies and Tools (CERTS). CERTS is an evaluation method that uses metrics to determine the suitability of a risk management methodology or methodological tool for a particular organizational situation. It was developed by Major William M. Garrabrants and Major Alfred W. Ellis III both from the Computer Technology Curriculum, Naval Postgraduate School (Garrabrants and Ellis, 1990). The motivation behind their work is to develop a methodology for comparing the large number of risk management methodologies and tools available today. These methodologies and tools were developed largely as a result of the decentralization of automated data processing (ADP) systems and the increased breadth of the information stored in the systems. As Professor Lance Hoffman noted in the 1986 National Computer Security Conference:

One significant lack today is metrics for risk analysis and risk management. There is no currently accepted set of criteria against which all methods can be compared. It is difficult to evaluate or to convey the advantages and disadvantages of a given methodology or tool when no

accepted evaluation metric exists. (Hoffman, 1986, p. 157)

With the development of CERTS, an effort has been directed toward the establishment of metrics for the evaluation of risk analysis and risk management methods and the appraisal of the numerous automated risk management tools currently available.

B. THE CERTS APPROACH

As stated above, the major objective for developing CERTS was to develop a new technique to effectively and objectively evaluate available risk management methodologies and tools for organizations and to establish a means of comparing these methodologies and tools. Garrabrants and Ellis concluded, through their preliminary research, that risk analysis criteria are a vital component of the selection of any risk management procedure. Their research lead them to believe that metrics could provide the means to measure a tool or package for suitability, thus assisting the user in selecting the most appropriate methodology for a given situation. This belief solidified their ultimate objective in establishing a standard set of metrics that could be used to evaluate risk management methodologies and tools for an organizational situation.

During the initial approach to this study, they discovered there was no existing technique to compare the risk management methodologies. Therefore, they developed an example of a

model, a paradigm, that promoted the comparison of risk management methods utilizing factors such as suitability, quality or acceptability. The ultimate purpose of this approach was to remove the analysts' deficiencies or biases from the evaluation, thereby assisting the analyst in determining which methodology should be selected.

1. A Measure for Suitability

Technology has brought an abundance of new risks that must be understood and addressed within the risk management arena. Businesses, companies, federal agencies, and all users of computer technology must be able to plan and forecast for the probability of adverse events. Numerous quantitative and analytical methods for risk management and decision-making under uncertainty have been developed, but the question still remains, "Which method is best for a particular situation?"

At this point the authors established a list of prerequisites a risk manager must possess in order to successfully accomplish this task. This list addressed the necessity of understanding the system being managed, its suitability to the purpose of the organization, and a thorough understanding of a majority of the methods available. Several risk management methods were found to be available for determining risks. Among those reviewed were Quantitative, Checklist, Scenario, Questionnaire methodologies, and hybrids

of each. The results revealed that each method has its own strengths and weaknesses that depend on the nature of its use.

2. Steps for Suitability

Garrabrants and Ellis concluded in their literature research that a great deal of effort had gone into the development of risk management methodologies, but that the methodologies lacked criteria and standardization. The application and development of their criteria for evaluation of computer security risk management methodologies followed those of Merkhofer (Merkhofer, 1987), but differs in the introduction of metrics which reduce the subjectivity of the criteria.

The next question to be addressed is how suitability would be defined. Suitability is defined as those characteristics of a risk management methodology or tool that are pertinent and appropriate for the requirements of a particular person, organization, system, and/or situation (Garrabrants and Ellis, 1990). The steps to measuring suitability is summarized in Table 1.

By implementing these steps, the analysis of suitability became standardized, flexible, and expandable. All criteria could now be compared consistently across all methods and could provide the user with the capability of expanding and weighing the criteria to meet his requirements.

This process resulted in the culmination of seven criteria composed of between two and four attributes. The criteria are: consistency, useability, adaptability, feasibility, completeness, validity, and credibility. (See Table 2.)

TABLE 1. STEPS FOR MEASURING SUITABILITY

1. Establish a set of criteria that describes a method's suitability.
2. Define the suitability criteria in terms of related attributes.
3. Specify metrics that describe the presence of the attributes.
4. Make a quantitative statement of the appearance of the suitability criteria by determining the ratio of actual occurrences of the metric to the number of possible occurrences.
5. Use the derived quantitative values for each of the criteria to evaluate and compare the variety of methods and tools available to the organization.

C. CRITERIA, ATTRIBUTES, AND METRICS

Once the seven criteria were developed, the authors selected the unweighted normative relationship model to formulate a simple mathematical relationship between the metrics and their associated criteria. The derived measurements of each attribute were viewed as a set, applied to a mathematical expression in boolean terms, and expressed as a ratio. In turn, each attribute within a criteria was summed to determine the ratio for that criteria. After

determining each criteria's ratio, the ratios were summed and applied to a mathematical expression resulting in a suitability index ratio.

TABLE 2. SUITABILITY CRITERIA

<p><u>Consistency.</u> Given a particular system configuration, results obtained from independent analysis will not significantly differ.</p>
<p><u>Useability.</u> The effort necessary to learn, operate, prepare input, and interpret output is generally worth the results obtained.</p>
<p><u>Adaptability.</u> The structure of the method or tool can be applied to a variety of computer system configurations (and the inputs can be easily updated as they periodically change).</p>
<p><u>Feasibility.</u> The required data is available and can be economically gathered.</p>
<p><u>Completeness.</u> Consideration of all relevant relationships and elements of risk management is given.</p>
<p><u>Validity.</u> The results of the process represent the real phenomenon.</p>
<p><u>Credibility.</u> The output is believable and has merit.</p>

Throughout the process of developing the criteria, their associated attributes, and metrics, the authors came to the conclusion that not all of the criteria could be maximized simultaneously. Some criteria are maximized at the expense of others. Thus, determining the best risk management tool or method would require trading one desirable trait for another. Therefore, the suitability of a method could be determined only after integrating the needs of an organization with the process as developed in this thesis.

1. Application of the Metrics

Now that a means of evaluating the suitability of risk management methodologies existed through the utilization of metrics, the method was augmented. To gain an appreciation of their validity, Garrabrants and Ellis applied their metrics to four sample, intuitively understandable methods of risk analysis. The four methods included: Annual Loss Expectancy (ALE), checklist, scenario, and questionnaire.

Using this approach, intuitive predictions were made for each of the criteria. The purpose of analyzing their results in the context of their predictions was to provide an approximation of the usefulness and integrity of the metrics. In essence, this process confirmed the metrics evaluation technique by providing an acceptable, standardized measurement of a methodology's attributes upon which to base a more sophisticated comparison of risk management tools.

The significance of the metric evaluation is in its application to hybrid methodologies. Hybrid methodologies are representative of the majority of tools that are currently available to computer security risk managers. The strength of the metrics evaluation technique was demonstrated by evaluating and comparing a small sample of four hybrid tools.

2. Performance of the Metrics

The evaluation results were focused on three different perspectives. These perspectives consisted of examining the

results of each tool separately, examining the results of each tool in comparison to each other, and finally, examining the results by comparing the suitability index of each tool.

D. CONCLUSION

Garrabrants and Ellis established a standardized set of metrics in a structured relationship that may be used to evaluate risk management methodologies and tools for their suitability in a given organizational situation. The metrics were successfully applied to four computer security risk management methodologies to develop an informal validation. The metrics were also used to evaluate four hybrid computer security risk management tools as a test and demonstration of the multiple criteria evaluation method. Its versatility was exemplified by the successful application to dissimilar tools. Several suggestions for extension of the concepts developed in their research were provided to guide future research.

III. THE ANALYTIC HIERARCHY PROCESS

A. INTRODUCTION

The Analytic Hierarchy Process (AHP) is a theory for modeling unstructured problems in the economic, social, and management sciences. AHP was developed by Thomas L. Saaty of the Wharton School, University of Pennsylvania (Saaty, 1980). AHP models a decision process as a hierarchy or a system of stratified layers, with the top layer being the ultimate goal or decision that needs to be made, and each succeeding layer being the criteria, subcriteria, subsubcriteria, etc. of the hierarchy. Finally, the leaf nodes represent the alternatives of the decision process. A pairwise comparison is made on each level of the decision tree to determine the importance of criteria and subcriteria, as well as the preference of the alternatives with respect to these criteria.

AHP is designed to consider as many relevant facts and ideas as possible to assist managers who have difficult decisions. When making these difficult decisions, managers normally consider the two or three major elements of a complex decision. Quite often other elements which play an integral role in the decision process may not be able to be considered. The AHP process helps to alleviate this oversight.

Pairwise comparison in AHP is more advantageous than the process of assigning weights. When assigning weights, all criteria are considered together with the most important criteria assigned the highest weight. This weighting process is used in assigning weights for all the succeeding ranked criteria. In pairwise comparison, each criterion is compared against each and every criterion to determine which criteria is most important of the two and by how much. The AHP process automatically calculates the weights for each criteria.

Once the hierarchy is established it may easily be modified. The manager does not have to start from scratch. New branches may be added to the hierarchy, and the comparisons remade. If a branch in the hierarchy attains a higher level of importance, the pairwise comparisons may be reevaluated with a bigger weight assigned by the process to that branch.

B. THE AHP PROCESS

The first step in setting up the AHP is to construct the hierarchy. Hierarchies are developed by the decision maker by establishing the necessary criteria to be considered. The hierarchy may be established from the top down or the bottom up. When a level becomes too complex or may not be readily compared, the element of that level may be broken down into newer lower levels, with finer distinctions. Even after this hierarchical development, modifications may be made by adding

new nodes (e.g., criteria, subcriteria, alternatives) to the decision process model.

The top level of a hierarchy is called the focus or the broad overall objective. The second layer represents the major criteria used in making the decision. Subsequent layers are subcriteria that further explain the major criteria. The leaves or bottom nodes of the tree are the alternatives from which the decision maker wants to select in order to accomplish the objective of the decision problem. Each layer may have numerous elements, although Saaty states that five to nine is an appropriate amount.

Figure 1 is a simple example of a hierarchy. The focus or the overall objective of the hierarchy is to select the best job. The second layer consists of the criteria used in making a decision. For this example, they include wage, location, and potential. The third and final layer in this example represents the alternatives available to the decision maker. In this example, they are IBM, APPLE, and NCR. Changes may readily be made to the hierarchy by adding new alternatives, such as Compaq, or by adding, deleting, or changing factors to be used in the determination of the job to be selected. For example, benefits could be substituted for potential in the hierarchy. The process of selecting a job for decision making may require a complex hierarchy. Every possible element relevant to the selection process should be included in the

hierarchy in order to allow the best possible decision to be made.

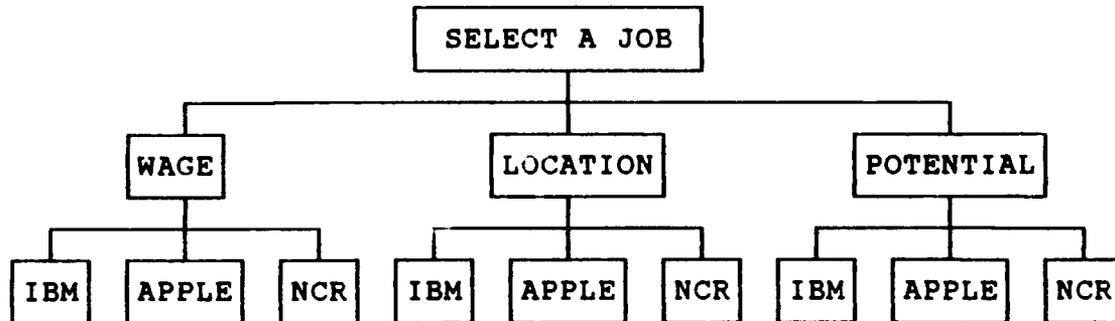


Figure 1. Select a Job Hierarchy

The second step in AHP consists of establishing or setting priorities among the elements of the hierarchy. The setting of priorities is established by pairwise comparisons within each layer of the hierarchy. Each comparison in the hierarchy is assigned a number from one to nine, with one being the items are of equal importance and nine being the one element having absolute importance over the other. The judgement of the ranking and importance of the items is at the discretion of the individual performing the comparison. Other values are dispersed between those two extremes. Pairwise comparisons may also be made using number or language (letters or verbal) assignments, depending on the preference of the user. Terms such as weakly more important, strongly more important, or absolutely more important may assist in the development of

complex pairwise comparisons. Table 3 shows the complete breakdown of the pairwise comparison criteria for AHP.

Comparisons of elements within a hierarchy may be made by placing the results into a matrix. The matrix format is based upon the number of elements in the hierarchy. The matrix of the example of Figure 1 is a three by three matrix, as shown in Table 4. An important question when making pairwise comparisons is:

How much more strongly does this element ... possess - or contribute to, dominate, influence, satisfy, or benefit - the property than does the element with which it is being compared? (Saaty, 1982, page 77)

The individual uses his judgment, knowledge, or his awareness of the situation to assign these values. The first comparison in Table 4 is made between wage and location. In this particular example, wage is assumed to be weakly more important than location, and therefore, a value of three was assigned, as indicated in Table 3. The reverse of this comparison, i.e. location to wage, has a reciprocal value of the wage to location comparison weight, or 1/3. The element in the left hand column of the matrix is always compared to the element in the top row of the matrix. The intensities are determined by the decision maker, through pairwise comparison, judgment, knowledge, or his particular awareness of a given situation. Wage has been demonstrated to be strongly favored to slightly dominant when compared to potential. Thus a

TABLE 3. THE PAIRWISE COMPARISON SCALE (Saaty, Decision Making for Leaders, page 78)

Intensity of Importance	Definition	Explanation
1	Equal importance of both elements	Two elements contribute equally to the property
3	Weak importance of both element over another	Experience and judgment slightly favor one element over another
5	Essential or strong importance of one element over another	Experience and judgment strongly favor one element over another
7	Demonstrate importance of one element over another	An element is strongly favored and its dominance is demonstrated in practice
9	Absolute importance of one element over another	The evidence favoring one element over another is of the highest possible order of affirmation
2,4,6,8	Intermediate values between two adjacent judgments	Compromise is needed between two judgments
Reciprocals	If activity i has one of the preceding numbers assigned to it when compared with activity j, then j has the reciprocal value when compared with i	

figure of six is assigned, and the reciprocal potential to wage is assigned a 1/6. The complete matrix is shown in Table 4.

TABLE 4. SELECT A JOB COMPARISONS

Element	Wage	Location	Potential
Wage	1	3	6
Location	1/3	1	3
Potential	1/6	1/3	1

The next step, termed synthesis (Saaty, 1982) is to set the overall priorities for a decision problem. Synthesis is the pulling together of all the values and arriving at one number to indicate the priority of that element. Table 5 illustrates this step in the synthesis of results of Select a Job Model. The columns of the matrix are totaled, and each entry in the column is then divided by the total of that column to obtain a normalized matrix, as shown in Table 6. This process allows comparison among the elements.

The average of each row is then computed by taking the sum of each row and dividing this sum by the number of entries in that row, as shown in Table 7. This gives the percentage of the overall priority for each element.

In this particular example, the wage criterion is the element which will have the largest impact on the decision on which job to take, as it is has the highest value.

An important item to consider is the consistency of the matrix derived through pairwise comparisons. An inconsistency could be introduced if, for example, an individual prefers the IBM job over the Apple job, the Apple job over the NCR job, but the NCR job over the IBM job. The overall consistency of the pairwise comparison matrix can be computed by means of an inconsistency ratio. The inconsistency ratio does not need to be exactly zero. If the value obtained is under 10%, then the pairwise comparison matrix is considered to be consistent. If the ratio is over 10%, then the pairwise comparisons are considered to be inconsistent and should be reevaluated.

TABLE 5. SYNTHESIS OF SELECT A JOB

Element	Wage	Location	Potential
Wage	1	3	6
Location	1/3	1	3
Potential	1/6	1/3	1
	1.5	4.33	10

TABLE 6. NORMALIZED MATRIX OF SELECT A JOB

Element	Wage	Location	Potential
Wage	.67	.69	.6
Location	.22	.23	.3
Potential	.11	.08	.1

TABLE 7. OVERALL PRIORITIES FOR SELECT A JOB

Element	Wage	Location	Potential	
Wage	.67	.69	.6	=1.96/3 = .65
Location	.22	.23	.3	=0.75/3 = .25
Potential	.11	.08	.1	=0.29/3 = .10

Consider the scenario shown in Table 8. In this scenario, wage is weakly more important than location and potential. Location is weakly more important than potential. The percentage of overall relative priorities is determined and presented in Table 9.

TABLE 8. MATRIX FOR INCONSISTENCY RATIO CALCULATION

Element	Wage	Location	Potential
Wage	1	3	3
Location	1/3	1	3
Potential	1/3	1/3	1
Column Totals	1.66	4.33	7

To determine if an inconsistency has been introduced into the decision process, each column value is multiplied by the relative priority for that criterion, i.e., the wage column with the wage priority of .57. The entries in each row are then totaled as shown in Table 10. Each row sum is divided by its corresponding relative priority as shown in Table 11.

TABLE 9. PRIORITIES FOR INCONSISTENCY RATIO CALCULATION

Element	Wage	Location	Potential	Row Sums	Average Row Sums
Wage	1	3	3	1.72	$1.72 / 3 = .57$
Location	1/3	1	3	0.86	$0.86 / 3 = .29$
Potential	1/3	1/3	1	0.42	$0.42 / 3 = .14$

TABLE 10. INCONSISTENCY RATIO CALCULATIONS

Element	(.57) Wage	(.29) Location	(.14) Potential	Row Total
Wage	.57	.87	.42	1.86
Location	.19	.29	.42	0.90
Potential	.19	.10	.43	0.43

TABLE 11. INCONSISTENCY RATIO CALCULATIONS

Wage	1.86 divided by 0.57 = 3.26
Location	0.90 divided by 0.29 = 3.10
Potential	0.43 divided by 0.14 = 3.07

The results of this division are summed then divided by the number of elements in the matrix to obtain the average. From this average the number of elements are subtracted and the result is divided by two. This is called the consistency index (CI) (Saaty, 1982). The CI in this example is 0.07. The inconsistency ratio is obtained by dividing the CI by an

average consistency, based on the number of criteria in the matrixes. The average consistency value for a matrix of three criteria is 0.58 (Saaty, 1982). The inconsistency ratio for Select a Job is .12 or 12%, which is above 10%, indicating an inconsistency in the pairwise comparisons. The pairwise comparisons should be reevaluated.

C. CONCLUSION

By using AHP, an individual may consider many more elements than is usually possible in the normal human decision thought process. An individual thought process can generally consider two to three factors, but with AHP, any number of factors can be considered. Even trivial elements which could have an impact upon the decision maker may be considered. Using a pairwise comparison, more accurate weights are calculated for the criteria, resulting in a more refined decision.

IV. IMPLEMENTATION OF CERTS USING THE ANALYTIC HIERARCHY PROCESS

A. INTRODUCTION

The purpose of this chapter is to adapt the CERTS method to the AHP process, and to develop a decision support system (DSS) to assist organizations in the selection of a risk management methodology or tool to suit their needs.

The CERTS technique is useful to an organization in the selection of a risk management package. However, this technique is hard to apply in its present form. Users must analyze a large number of questionnaires, then perform the necessary computations manually to determine the best available package. CERTS does not have the ability to differentiate strengths and weaknesses of certain metrics, as it makes boolean determinations only. Weights may not be assigned to these criteria to further refine the solution to address the priority needs of the organization. The application of CERTS is also tedious and time consuming for the user. CERTS application requires that the user become thoroughly familiar with each risk management package being analyzed.

The AHP process, however, assists in overcoming these problems. The process is completely automated, decreasing the amount of time required to fill out questionnaires with the

calculations being done automatically. The pairwise comparisons of AHP allow the assignment of weights to criteria, attributes and metrics. The user will not have to become intimately familiar with each package as weights could be assigned to each package in the leaf nodes.

The DSS selected to incorporate CERTS into AHP was Expert Choice, developed by Expert Choice, Incorporated of Pittsburgh, Pennsylvania. Expert Choice offers the capability of a hierarchy up to six levels deep, with up to seven subnodes for each node of the hierarchy. Pairwise comparisons may be made at each level. Expert Choice can therefore support a decision process with thousands of input criteria.

B. IMPLEMENTATION OF CERTS USING AHP

The CERTS methodology is readily adaptable for implementation using AHP. The concepts of criteria, attribute, and metric in CERTS map nicely into the concepts of criteria, subcriteria, and subsubcriteria in AHP. This is explained in the following paragraphs.

The objective of selecting the best risk management package becomes the top layer or goal of the AHP hierarchy. The CERTS criteria level becomes the second layer of the hierarchy. These are the main decision elements of the DSS and are shown in Figure 2. The third level of the hierarchy contains the attributes that are used to refine the criteria. These attributes correspond to the subcriteria of the AHP

method. The fourth level of the hierarchy contains the metrics that are used to further define the attributes. These metrics expressed as questions in CERTS were modified and expressed as subsubcriteria in the AHP hierarchy. These subsubcriteria could be used in pairwise comparison, and, therefore, assigned weights. For example, the boolean metric for the subcriteria reliability, "Does the process provide a mechanism to reduce the introduction of personal bias?" is transformed into the subsubcriteria of "reducing the introduction of personal bias." Then "reducing the introduction of personal bias" may be compared with other subsubcriteria and assigned a weight. Each criteria is discussed in detail in the sections below. Finally, the leaf nodes of the hierarchy contains the alternative risk management tools from which the most appropriate package will be selected. Incorporating the alternatives in the hierarchy is explained in Section C.

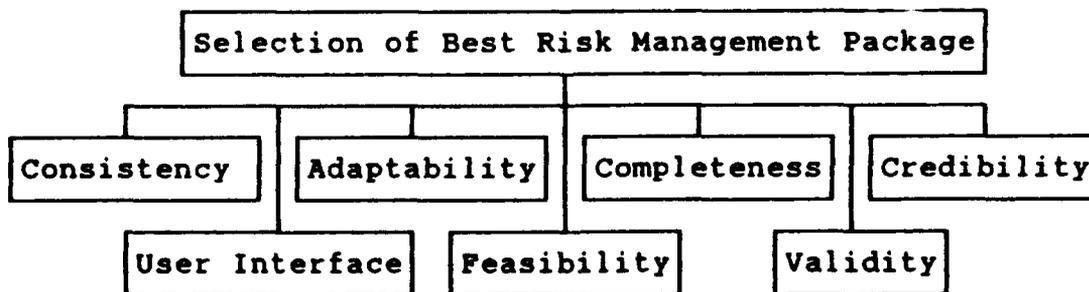


Figure 2. Criteria of Risk Management Package Hierarchy

1. Consistency

Consistency relates to the ability to duplicate the results consistently throughout the process. Consistency has subcriteria of reliability and consistent terminology. Reliability is concerned with a package's objectivity or the reduction of subjectivity in the risk management process. The subcriteria of consistent terminology relates to the ability of the package to use the same terminology throughout the entire risk management program. The subcriteria and subsubcriteria for consistency are listed in Template 1 of Appendix A.

2. User Interface

User interface is the ability and knowledge needed by the user to understand the complete system, as well as the level of support provided by the vendor of the system. The criteria of user interface is broken down into subcriteria of error handling, simplicity, ease of use, understandability, and support. Error handling is concerned with the ability of the program to identify input errors. Simplicity deals with the outward appearance of the package, e.g., does it appear easy for the user to understand the process. The ease of use subcriteria measures how well structured and logically sequential the process is. Understandability relates to the ability of comprehending the underlying premise that supports the package methodology. Support is concerned with the

assistance provided by the program vendor. The subcriteria and subsubcriteria for user interface are listed in Template 2 of Appendix A.

3. Adaptability

Adaptability relates to the ability to apply the method to various types of computer systems, and whether it may be easily updated. Computer systems run the gamut from personal computer to mainframe computer to a complex distributed network. Adaptability has the subcriteria of portability and modifiability. Portability is concerned with the ability to use the product across various computer systems and configurations. Modifiability is the ability to apply different alternatives or options to the process to determine the effect upon the outputs. The subcriteria and subsubcriteria for adaptability are detailed in Template 3 of Appendix A.

4. Feasibility

Feasibility is concerned with the cost and amount of effort required by the organization to fulfill the information requirements and input for the risk management package. Subcriteria for feasibility are availability, practicality and scope. Availability subcriteria distinguishes between internal and external data needed by the system, and the ease by which that data may be obtained. Concern with the economics of gathering the required data is covered by the

subcriteria of practicality. Scope deals with the broadness of the system to cover all necessary items contained in the organization's information. Template 4 of Appendix A presents the subcriteria and subsubcriteria for feasibility.

5. Completeness

Completeness is concerned with the coverage of all risk management areas of concern to the satisfaction of the user. Scope, elements, and element attributes are the subcriteria for completeness. Scope, which is duplicated in other criteria, is concerned here with the level of detailed analysis that is done throughout the various aspects of the organization. Elements deal with the components that operate to determine the risks of a system. Subcriteria of completeness are concerned with the outcomes or consequences that could occur from the elements attributes. The subcriteria and subsubcriteria of the completeness subcriteria are shown in Template 5 of Appendix A.

6. Validity

The validity criteria measures the package's ability to represent reality of desired legitimate situations. The subcriteria for validity are relevancy, scope, and practicality. Relevancy means that results of the process are meaningful to the organization. Scope is used in the context of validity of the process on all the various aspects of the organization. Practicality is repeated again from the

feasibility criteria, but deals with the validity of the data gathered by the process. Template 6 of Appendix A displays the criteria and subsubcriteria of the validity criteria.

7. Credibility

The last criteria, credibility, deals with whether the conclusions arrived at by the package are acceptable by the organization. The subcriteria of credibility are intuitiveness and reliability. Intuitiveness shows whether the results will instill and maintain the confidence of the user organization. The ability to obtain repeatable results from the package determines the reliability. Template 7 of Appendix A exhibits the subcriteria and subsubcriteria for the credibility criteria.

Appendix B shows the output from Expert Choice implementing CERTS.

C. INCORPORATING ALTERNATIVES TO THE HIERARCHY

1. Alternative Risk Management Packages

The alternative risk management packages were selected in conjunction with inputs from the Department of Commerce's National Institute of Standards and Technologies (NIST). The risk management packages for this study were selected from data obtained from the sampling and extensive testing of numerous risk management packages at NIST's Risk Management Laboratory. The packages that were selected were LAVA, developed by Los Alamos National Laboratory, Los Alamos, New

Mexico; BDSS, developed by Ozier, Perry and Associates, San Francisco, California; and RISKWATCH, developed by Expert Systems Software, Incorporated, Long Beach, California. These packages became the leaf nodes of the AHP hierarchy.

The subsubcriteria in the lower level of the Decision Support System, (listed in Templates 1 through 7 of Appendix A) were applied to the three packages. The ability of each risk management package to meet the subsubcriteria was measured by the authors and NIST personnel's qualitative opinions.

2. Assigning Weights to the Alternatives

Using pairwise comparison, each risk management package was assigned a weight that indicates its preference with respect to each subsubcriteria. If two packages were deemed equal in ability by the authors, then the DSS assigned equal weights to these packages. For example, it was found that in Template 1 of Appendix A, the subsubcriteria "establishing standard language" of the subcriteria consistent terminology, of the consistency criteria, was addressed equally by all three packages (LAVA, BDSS, and RISKWATCH). Therefore, pairwise comparisons assigned equal weights to each package. This is shown in Table 12.

Pairwise comparisons were made for all subsubcriteria for the DSS. As described in Chapter II, Table 1, comparisons may be made by numerical, or verbal methods. In addition, DSS

offers a graphical means of presenting the pairwise comparison in the form of a pie graph. An example of weights resulting from a pairwise comparison is shown in Table 13 for the criteria "consistency," the subcriteria "reliability," and for the subsubcriteria "reducing the introduction of personal bias." Verbal comparisons were made of the alternative risk management packages such that LAVA was deemed to be moderately more important than BDSS and equal to moderately more important than RISKWATCH, while RISKWATCH was deemed to be equal to moderately more important than BDSS. Appendix C shows all pairwise comparison results for the alternatives in regard to the subsubcriteria.

TABLE 12. EQUALITY IN PAIRWISE COMPARISONS

Criteria: Consistency
 Subcriteria: Consistent Terminology
 Subsubcriteria: Establishing Standard Language

Risk Management Packages	DSS Assigned Weight
BDSS	.333
LAVA	.333
RISKWATCH	.333

The inconsistency ratio is automatically calculated by the DSS for each set of assigned weights. The inconsistency ratios were under 10% for all pairwise comparisons of the risk management packages. The comparisons were thus deemed to be free of inconsistencies.

In the next chapter we apply the developed DSS to three hypothetical case studies.

TABLE 13. WEIGHTED ALTERNATIVES SCORES

Criteria: Consistency
Subcriteria: Reliability
Subsubcriteria: Reduces the Introduction of Personal Bias

Risk Management Packages	DSS Assigned Weight
BDSS	.163
LAVA	.540
RISKWATCH	.297

V. APPLICATION OF THE DSS TO CASE STUDIES

A. INTRODUCTION

In Chapter IV, the CERTS methodology was applied to the AHP method to develop the CERTS Decision Support System (DSS). This DSS may then be used by an analyst to determine the best risk management package for a particular computer system site or situation. This chapter demonstrates the application of the DSS to three different hypothetical case scenarios. These case studies were provided by NIST and further developed by the authors.

1. Application of CERTS DSS

The choice of a suitable risk management package depends upon the experience of the analyst and how well he tailors the organizational requirements to the evaluation. The CERTS DSS could be an invaluable tool in assisting the analyst in determining the best package to use. For the purpose of this thesis, CERTS DSS includes three risk management packages. Additional packages could be incorporated easily in the AHP hierarchy using the approach detailed in the previous chapter.

The procedure to apply the CERTS DSS for each case is simple, systematic, and straightforward. Initially, the analyst conducts pairwise comparisons of the seven criteria at

the first level of the DSS, according to the organization's particular needs. Consequently, the system assigns weights to the various criteria. The analyst may refine the selection process by further conducting pairwise comparisons of the subcriteria and subsubcriteria of each criteria in the hierarchy.

Upon the completion of each level of pairwise comparisons, the system calculates an inconsistency factor. If the factor is over 10%, then some type of inconsistency exists. The pairwise comparisons should then be reviewed and reconsidered until the inconsistency ratio is below 10%. Once the weights have been assigned, the synthesis is conducted to derive the overall results. The program calculates an overall weight for each risk management package based on the pairwise comparisons made by the analysts. The program with the highest weight is, therefore, the most suitable for the organizational situation.

2. Disclaimer for Case Scenarios

The case scenarios presented are modeled after test cases provided by the Risk Management Laboratory at the National Institute of Standards and Technology. The information provided by the cases should not be construed to represent actual circumstances, conditions, or procedures of any kind that may exist in any actual site. The cases were developed and designed to provide as realistic and consistent

input as possible to the CERTS DSS for the evaluation of the risk management packages.

B. CASE SCENARIO DESCRIPTIONS

1. Case Scenario One: Distributed Wide Area Network (WAN)

System X is a nationwide distributed office automation and work/project tracking system. The system provides word processing, electronic mail, spreadsheets, databases, and graphics. In addition to performing its network functions, the database serves as a management information system.

This information system provides management with computer listings of the daily and overall functions of each office. All work projects are tracked on the database. Tracking is required for the allocation and purchase of resources. The workload is primarily in the format of word processing documents. Databases and spreadsheets are used to support this function.

a. Physical Environment

The system is distributed over nine sites. The headquarters (HQ) is located in a Northeastern city, with other sites spread around the U.S. at field centers (FCs). At HQ, the system is linked via two leased lines to the mainframe complex. Each of the FCs' computers is linked into its center LAN. All the sites are connected via a network that runs on the agency's telecommunications system using a public packet

switching service. Backup service at the HQ minicomputer is provided for the dial-up access. Access to the HQ mainframe is through a packet-switched network to the HQ minicomputer. The minicomputer functions as a file and print server for the office.

b. Equipment

The dollar value of equipment is as follows:

200 micros @ \$3,000	\$600,000
8 small minicomputers @ \$75,000	600,000
1 medium minicomputer @ \$200,000	200,000
25 laptops @ \$2,000	50,000
misc. printers, modems, etc.	<u>100,000</u>
TOTAL	\$1,550,000

Equipment used but not owned include: (by contractor) packet-switched network; leased lines between HQ mini and mainframe computers; and internal networks of various types at the different sites. The communications equipment is five years old.

c. Personnel

All personnel receive critical-sensitive background checks before employment. A few administrative personnel receive national agency checks (NAC). The management has no policy on separation of duties.

There is no computer security training. However, workers are informed of their physical security responsibilities, which include: displaying their picture badge at all times; challenging any person not wearing a badge

for whose activity or presence appears questionable; reporting the loss or misuse of a badge; and surrendering a badge when it is no longer needed. A computer security person has been assigned by management to track this function.

There are 300 people at HQ. Each of the FCs have between 100 and 150 people. Resource protection measures at all sites include: fraud, waste, and abuse education of personnel; marking of all equipment; maintaining an active inventory of all hardware and software; and making personnel responsible for protection of government property. There are attractive features (e.g., full color printing) in the system, but no games are allowed. Staff working outside normal hours are unsupervised.

d. Data Environment

One database is run on the HQ mainframe computer and several are run on the HQ minicomputer. Access to the HQ mainframe computer is accomplished via a packet-switched network, which allows transmission from the HQ minicomputer to the mainframe computer over two leased lines. Backups are made nightly of the HQ minicomputer and mainframe computer; these tapes are stored off-site on a weekly basis. Backups of the PCs are made by individual staff members.

The data is highly sensitive. Accuracy and timeliness of the data is required for monthly and semiannual reporting. Inaccurate data would result in poor planning and

mismanagement of resources. Some of the data requires stringent confidentiality protection due to privacy laws. Disclosure of this data would result in mission failure, dollar loss to the agency, possible lawsuits, and embarrassment to the organization. The disclosure, however, would not seriously affect the agency mission. Losses for disclosure could be \$500,000 to \$1 million, excluding the cost of lawsuits. Losses for mismanagement could be quite costly.

e. Operating Systems

The system cannot be described as 'hacker friendly'; there is a warning screen when signing onto the HQ mini- and mainframe computers. The communications equipment has not been specially adapted for any site. Remote site dial-up users accessing the system receive full processing capability. It is not easy to 'crash' the applications software and break into the operating system or other applications. On the other hand, untested software from vendors for trial processing is often allowed. This is a potential for vulnerability, since no virus detection software is available on the system.

The mini- and mainframe computers have access control with passwords, which allow for three tries before locking the user ID. Passwords are required to be changed every 90 days. Passwords on minicomputers are four characters long; passwords on mainframe computer are six to eight

characters long. Passwords for both the mini- and mainframe computers are: suppressed automatically during entry; intentionally related to the user's identity, history, or environment; replaced with a new password when forgotten; and generated by the user. Management policy prohibits the use of group passwords. Passwords and user IDs are removed from the minicomputers promptly when an employee leaves. There is no timeout on unused accounts.

Loss of availability of the system for short periods (one day) is not a major problem. The loss of the large minicomputer for a day, the loss of network, the mainframe computer, or the small minicomputer for more than seven days would significantly affect productivity. This time loss could result in missed mandated monthly and semiannual deadlines. Approximate loss of productivity is \$500,000 per week. The loss of the mainframe computer for a week or more or the loss of the network at a critical reporting time would result in failure to meet legislated or administrative deadlines. While this would produce no dollar loss, goodwill would be lost and future budget considerations would suffer. The loss of the FCs or HQ for more than a week would be disastrous to the agency. The monetary cost would be the equipment cost plus loss of productivity at \$200,000 per week per site.

Audit and variance detection are implemented. The audit trail is read often and handled in a timely manner. A

security person checks all unsuccessful logins and system bugs. Although technical controls consist of authorization/access control, audit trail mechanisms, an encryption package, error checking/correcting protocols, and user ID and authentication, there is no form of message authentication code (MACing) on this system.

One case of deliberate misuse of resources by authorized staff last year was detected at one of the FCs. The average level of staff experience with the system is more than two years. The turnover in staff averages 15% per year. The approximate number of non-staff personnel (e.g., visitors, contractors, maintenance) entering the headquarters or supporting facilities each day is 50.

f. Management Philosophy and Concerns

Top management, along with selected members of a risk management assessment team, convened to determine their major concerns in the selection of a risk management tool with the intention of using the CERTS DSS. The committee used the pairwise comparison of the DSS to establish their priorities for the criteria. Table 14 shows the rankings and summarizes the weights assigned to the criteria by the DSS. As Table 14 indicates, user interface was deemed to be the most important criteria in selecting a risk management package. This was followed by adaptability, consistency, credibility, validity, feasibility, and completeness, respectively.

Since System X is a nationwide network and requires that each site apply the risk management application, user interface is a top priority consideration. With nine sites spread across the United States, importance is stressed on ease of use, comprehension, and developer support. The distance between sites has generated risk management concerns

TABLE 14. DISTRIBUTED WAN

Ranking	Criteria	DSS Assigned Weight
1	User Interface	.354
2	Adaptability	.240
3	Consistency	.159
4	Credibility	.104
5	Validity	.068
6	Feasibility	.045
7	Completeness	.031

in the areas of input preparation, execution of the process, and the interpretation of output. These concerns represent the interface and relationships between the analyst and the process. The users of the risk package are not required to comprehend all features of the process, but do need to understand what decisions are expected of them. A process that is well structured and logically sequential is critical to the ease-of-use aspect. Developer support must include complete and extensive documentation, 24 hour phone support,

and comprehensive on-site training. Table 15 provides the ranking and the DSS assigned weights for the user interface subcriteria.

Given this particular system configuration, adaptability is high on the list of management concerns. The search is for a package or tool that may be applied to a variety of computer system configurations. Portability is of utmost importance when dealing with a highly distributed environment, such as presented in this case. The package must apply to a changing environment, as the possibility of adding or deleting field sites is high. This change may trigger a need to modify the tool to assist the analyst in examining alternatives or options. Table 16 summarizes the rankings and the DSS assigned weights for the adaptability subcriteria.

TABLE 15. USER INTERFACE

Ranking	Subcriteria	DSS Assigned Weight
1	Ease of Use	.241
2	Understandable	.223
3	Support	.185
4	Simplicity	.178
5	Error Handling	.172

Standardization for risk management is required across the entire network. Therefore, the results obtained from the risk management package for each site should not be significantly different. Consistency implies the ability to

TABLE 16. ADAPTABILITY

Ranking	Subcriteria	DSS Assigned Weight
1	Portability	.570
2	Modifiability	.430

duplicate the results of the process. A key component of consistency is reliability. Reliability reduces the wide amount of variance that could occur as a result of personal biases. The more the process reduces biases in the analysis at each site, the more consistent the results will be between the analysis teams at each site. Table 17 depicts the rankings and weights assigned by the DSS for the consistency subcriteria.

TABLE 17. CONSISTENCY

Ranking	Subcriteria	DSS Assigned Weight
1	Reliability	.560
2	Consistent Terminology	.440

The data used over the WAN is highly sensitive. Losses for disclosure could run up to one million dollars. Consequently, the credibility aspect of the package is essential to the merit of the output. The reliability of the risk management package is also essential to its credibility. With the possibility of high monetary losses, the same results

must occur when the same data is used on different occasions. Table 18 shows the ranking for the credibility subcriteria.

The credibility of a risk management package is closely followed by the validity aspect of that package. Management wants to avoid the possibility of obtaining irrelevant conclusions or results. These results must be meaningful to the system. The process should also provide categories of solutions rather than specific recommendations. Table 19 presents the ranking for the validity subcriteria.

TABLE 18. CREDIBILITY

Ranking	Subcriteria	Score
1	Reliability	.540
2	Intuitiveness	.460

TABLE 19. VALIDITY

Ranking	Subcriteria	Score
1	Relevancy	.365
2	Practicality	.332
3	Scope	.303

The feasibility of obtaining the data is less important as each site does its own application. Completeness was also as a minor concern of risk management in this case. Therefore, the subcriteria within each of these criteria were

considered of equal importance. Tables 20 and 21 display the rankings and the weights assigned by the DSS for the feasibility and completeness subcriteria, respectively.

The CERTS DSS selected RISKWATCH as the best risk management package for the Distributed Wide Area Network (WAN) Scenario. The detailed results are shown in Appendix D, Templates 1 through 3.

TABLE 20. FEASIBILITY

Ranking	Subcriteria	DSS Assigned Weight
1	Availability	.333
1	Practicality	.333
1	Scope	.333

TABLE 21. COMPLETENESS

Ranking	Subcriteria	DSS Assigned Weight
1	Attributes	.333
1	Elements	.333
1	Scope	.333

One of the major advantages of the CERTS DSS is that you need not discard the whole framework if you find that you overlooked something in formulating the priorities of the criteria. The system is designed to show the sensitivity of each criteria to the alternatives. For example, if management desired to place more emphasis on consistency, for the above

case, the CERTS DSS would select LAVA as the best risk management tool for the Distributed Wide Area Network (WAN). The sensitivity analysis is illustrated in Appendix D, Template 4.

2. Case Scenario Two: Under Development System - Biomed

The Biomed system is a new system, currently being developed, that is designed to track biomedical research, including animal research. Applications will be developed to track and record results of experiments and will be used to write proposals and reports. The software will include relational and hierarchial database packages, word processing, and graphics packages. These packages will share data when creating reports and presentations.

a. Physical Environment

The Biomed system is currently under development and will be located in a single tenant government building in suburban Washington. The building has no fence and is accessible from the street. Site access is controlled by picture ID badges and 24 hour-a-day guards. Visitors with proper identification are allowed unescorted into the facility.

The site has a staff of 1,700. The Biomed system will be used by 100 local and 50 remote users. Approximately 75 non-staff personnel (e.g., visitors, contractors,

maintenance) enter the site each day. The turnover in staff averages 8% per year.

Each lab and office has a sprinkler system, which is part of the building system. All labs have hand-held fire extinguishers, but offices do not. All lab personnel have been trained in the extinguishers' use. No smoking is allowed in the building. Food and drink are discouraged, but not prohibited. Inflammable materials (e.g., solvents) are stored and processed at the site. Three fires have occurred in the labs within the last two years.

The Biomed system will be in an existing computer room with raised flooring, environmental control, heat detectors, drains, and fire suppression. The room is in the basement with no windows. Once a month, the floor beneath the raised floor is cleaned by a special crew.

b. Equipment

Based upon the functional needs and expected usage, a minicomputer or small mainframe computer will be procured. The expected value of minicomputer and operating system is \$150,000. Total cost of the application software is estimated at \$700,000. Existing PCs will be used to access the system.

c. Personnel

The agency provides national agency checks (NACs) for all employees. There is no computer security training. However, personnel are aware of their physical security

responsibilities, including: displaying the badge at all times; reporting the loss or misuse of a badge; and surrendering a badge no longer needed. Responsibility for computer security of the Biomed system will be assigned by management. Staff working outside normal hours are unsupervised.

d. Data Environment

The data requires strong integrity protection to ensure that published experiment results are correct. Availability is required for maximizing productivity. Brief down times will be inconvenient but not critical. The data is time-sensitive and is not made public until experiments and analysis are complete to avoid improper interpretation of results.

e. Operating Systems

On-site Biomed system users will access it through a LAN. The proposed method for remote users is through dial-in ports; 5 ports are anticipated. There are no dial-up communication lines now in place. The communications equipment will not be specially adapted.

f. Administration

The Animal Rights groups are an active threat. These groups have demonstrated at the site, and it is presumed they have skilled computer operators within the group. They have conducted raids against the site, destroying property and

releasing animals. City police are used during demonstrations. Forced entry into the building may be accomplished, however, forced access into the internal offices and labs is difficult.

As the Biomed system is under development, there are no operational or technical controls currently in place. There has been no emergency, backup, or contingency planning done for the proposed Biomed system. Backup is available for air conditioning and power. There will be attractive features (e.g., full color printing) available in the Biomed system, and games will also be on the system.

If the Biomed system is down for 24 hours, there will be no problem. If the Biomed system is down for 7 days or more, there will be a loss of productivity of \$40,000 per day. Two weeks is the maximum acceptable downtime for this system. After that, a loss of confidence will occur and could cause possible loss of future funding.

Since the data is used for biomedical research, compromises may be (but are not necessarily) related to a possible loss of human life through extended research time or improper authorization for human experimentation. Compromise could include: damage through error; unauthorized disclosure or modification; and unavailability of the Biomed system. There would be no monetary impacts (such as law suits), but compromise could result in failure to accomplish the agency

mission, improper interpretation of results, or loss of public confidence and future funding.

The Office of Scientific Integrity has a strong policy on maintaining the integrity of scientific projects. Management allows group data passwords only if they are known by authorized users. Management has in-place resource protection measures which include: marking of all equipment; maintaining an active inventory of all hardware and software; and making personnel responsible for protection of government property. Despite this, there have been three cases of deliberate misuse of resources by authorized staff in the last year. The staff is trained in emergency procedures which include: evacuation procedures; CPR training; first-aid kits on each floor; and health facilities at each site. The Biomed system procedures will be written after the system is procured and the applications are developed.

g. Management Philosophy and Concerns

During the design phase of the Biomed system, an automated data processing security branch was developed to address and direct all security issues associated with the project. Top management envisioned this branch as a key contributor to the development of the new system. To fulfill this requirement, the branch established a risk management team of technical, administrative, management, and programming experts. The team's initial mission was to select a risk

management package to assist in system development. The CERTS DSS was used to select this package, and pairwise comparisons were made for all the criteria. For example, completeness was deemed to be more important, in varying degrees, than any other criteria. The rankings and DSS assigned weights for pairwise compared criteria are summarized in Table 22. Completeness was followed by credibility, consistency, validity, user interface, adaptability, and feasibility, respectively.

The team's primary concern in the choice of a risk management package is to ensure completeness. The package must take into consideration all relevant relationships and system elements of risk management. Since the Biomed system is a new, under development system, top management is also concerned that the analysis considers all aspects of the system. Desired elements of coverage could include assets, threat agents, threat events, safeguards, vulnerabilities, and outcomes. This array of information is regarded as critical in the development of the DSS methodology and the satisfaction of the needs of the organization. The management desires that the relationships between the elements of risk are addressed in areas such as local and remote users, known activist threats, integrity of scientific projects, emergency situations, backup situations, and contingency planning. Table 23 displays the rankings and the DSS assigned weights for the completeness subcriteria.

Management tends to view the credibility of a particular method or package with utmost importance when involved with sensitive data. The process used has a significant bearing on the acceptability of its conclusions. The data produced in Biomedical research requires strong integrity protection to ensure that the results are correct. With the possibility of system compromises that could lead to the loss of human life, it is imperative that the risk package encompass all threats and vulnerabilities. The reliability of the method provides credence to those interpreting the output. If different results are returned using the same data on different occasions, the method will hold little plausibility for its users. Table 24 shows the rankings and the DSS assigned weights for the credibility subcriteria.

TABLE 22. BIOMED SYSTEM

Ranking	Criteria	DSS Assigned Weight
1	Completeness	.354
2	Credibility	.240
3	Consistency	.159
4	Validity	.104
5	User Interface	.068
6	Adaptability	.045
7	Feasibility	.031

TABLE 23. COMPLETENESS

Ranking	Subcriteria	DSS Assigned Weight
1	Elements	.401
2	Attributes	.320
3	Scope	.279

With the strong requirement for maximizing productivity and ensuring that published results are correct, consistency is the next criteria emphasized by management. Scientific research provides an atmosphere of constant change and various risks. When an analyst is evaluating these risks, he has a tendency to make inferences based on what he remembers hearing or observing. A key component of consistency, reliability, furnishes support for the reduction of subjectivity in the risk management process. Another concern in this process is controlling differences in interpretation. Interpretation is defined as the information being asked for versus what the product represents. A uniform set of terminology is a must between the analyst and the process. Table 25 depicts the rankings and the DSS assigned weights for the consistency subcriteria.

The validity of a package is exposed to the numerous impacts that the risks impose on the data. Equal concern was expressed for the subcriteria of validity. To maintain relevancy of the results, it was felt that the results of the package must therefore relate to significant

TABLE 24. CREDIBILITY

Ranking	Subcriteria	DSS Assigned Weight
1	Intuitiveness	.524
2	Reliability	.476

TABLE 25. CONSISTENCY

Ranking	Subcriteria	DSS Assigned Weight
1	Reliability	.550
2	Consistent Terminology	.450

areas of need and also incorporate mandated security requirements. The user of the package must be able to control the level of detail being analyzed and must also be able to consider all aspects of the system. Table 26 presents the rankings and the DSS assigned weights for the validity subcriteria.

TABLE 26. VALIDITY

Ranking	Subcriteria	DSS Assigned Weight
1	Relevancy	.365
2	Scope	.322
3	Practicality	.313

User interface was a minor concern, based on the experience and level of training of each member of the risk management team. The subcriteria of ease of use and

comprehension of underlying premises with methodology are a plus for this criteria. The team requires 24-hour phone support or a 1-800 number service. Table 27 provides the rankings and the DSS assigned weights for the user interface subcriteria. As the Biomed system procedures will be written after the system is procured, adaptability and feasibility are of less concern at the present time than other areas. Tables 28 and 29 summarize the rankings and the DSS assigned weights for the adaptability and feasibility subcriteria.

TABLE 27. USER INTERFACE

Ranking	Subcriteria	DSS Assigned Weight
1	Ease of Use	.419
2	Understandable	.263
3	Support	.160
4	Error Handling	.097
5	Simplicity	.062

The CERTS DSS selected BDSS as the best risk management package for the Biomed scenario. The detailed results are shown in Appendix E, Templates 1 through 3.

TABLE 28. ADAPTABILITY

Ranking	Subcriteria	DSS Assigned Weight
1	Modifiability	.530
2	Portability	.470

TABLE 29. FEASIBILITY

Ranking	Subcriteria	DSS Assigned Weight
1	Practicality	.460
2	Scope	.319
3	Availability	.221

As described in the first case, a sensitivity analysis can be performed if your priorities for the criteria change. If management decided they wanted a more portable package, additional weight would be applied to the adaptability criteria. With the newly assigned weight, the CERTS DSS would select RISKWATCH as the best risk management tool for the Biomed case. The sensitivity analysis is illustrated in Appendix E, Template 4.

3. Case Scenario Three: Data Center

The ABC Corporate Data Center supports the North American Operation, a subsidiary of United Corporation. The North American Operation has 400 full-time employees and is the fifth largest banking organization in the Northeast United States. The data center is responsible for processing checking accounts, savings deposits, loans, and savings certificates. Additional responsibilities include maintaining off-the-shelf personnel and management computer applications.

a. Physical Environment

Two buildings were converted for company use, ADP and Administration. The buildings are next to one another,

but not physically connected. The buildings are located in a large Northeastern American city on an average city street. A sidewalk runs along one side of each building. There is an adequately lit employee parking lot. The possibility of an earthquake in that area is low.

The ADP Building is a 20 year old warehouse and houses the mainframe computer and the tape library. Conversion improvements consist of: raised flooring to accommodate cables and wiring; suspended acoustical tile ceiling to absorb sound and hide the overhead plumbing; power distribution upgrade; surge suppression; lighting; and air conditioning and heating. There are no under floor water detectors or temperature-humidity recording systems. The roof is in good shape, despite its age. Recently, water stains have been noticed in other parts of the building. The concrete floor below the raised floor was last cleaned when installed five years ago.

The Administration Building was originally constructed as an ADP Center. Therefore, it is equipped with adequate environmental systems (similar to those of the current ADP building). When it was converted to its present use, an overhead sprinkler system was added to conform to fire codes. Neither building has an emergency backup generator. The power is supplied solely by the local power company.

b. Equipment

The Data Center contains an XYZ-3100 Mainframe with six tape drives, 12 disk drives, and 3 on-line printers, all located in the computer room of the ADP building. In addition, 20 terminals are located in an uncontrolled area of that building. These terminals are connected to the XYZ-3100 Mainframe via the data communication system. Despite a constant workload, the system only operates at 60% capacity. This low capacity is attributed to poor employee performance, software failure, and unreliable equipment. The equipment repairs are performed on a 'per incident' basis by a contractor hired on that basis. No regular maintenance is performed on the hardware. The Administration Building has PCs, however, none of the PCs lock or are secured to the furniture.

The dollar value of equipment is as follows:

1 mainframe computer @ \$350,000	\$ 250,000
6 tape drives	10,000
12 disk drives	150,000
30 personal computers	200,000
1 communications controller	10,000
2 modems	5,000
4 multiplexers	4,000
Other (paper, disks, printers, etc.)	<u>100,000</u>
TOTAL value of equipment	\$ 829,000

c. Personnel

Background checks are not performed on new hires. Only the 20 data entry clerks and 10 computer operators (of 50 employees) are considered essential to production operations.

However, excessive use of sick leave and a high rate of turnover is a problem with these essential employees. Personnel shortage, the continuing need for overtime, and excess sick leave adds to the backlog of work, which must be made up at time-and-a-half rates. The loss of an operator or clerk results in recruitment fees and training costs for replacement personnel. The average level of experience for the system staff is two years. The average percentage of turnover in staff per year is 40%.

No formal form of computer security training exists for personnel. The only existing training is for new data entry clerks on the performance of their jobs. There are no passwords for any system entry.

d. Data Environment

The Pay/Personnel and Financial/Management application systems are off-the-shelf and maintained by upgrades from the vendor. Company personnel trained on the software can make quick patches when necessary. These systems and data files constitute the critical work-load (80% of the total) of the Center. The rest of the work is general administration of the company, using standard business software. Backups are made once a week. These backups are stored in the tape library, with the original copy of the software. Backups are kept for three weeks before being recycled.

Data sensitivity is primarily based on its integrity requirement and is considered to be highly sensitive. The potential for loss, due to fraud or error, is high. The system controls 500 million dollars of disbursements annually, as well as a payroll. The availability of the system is required for operations and employee productivity and has medium sensitivity, since it can be accessed manually. A confidentiality requirement exists for personnel data on the system. This data is classified as medium sensitive due to the Privacy Act stipulations placed on government contractors.

e. Operating Systems

The proprietary system software is supplied by the hardware vendor and provides no controls to limit access to software or data files. Copies of the system software may be obtained from the vendor at no charge and made operational in approximately eight hours. A standard operating procedure is to obtain a clean copy of the operating system from the vendor whenever the on-site OSS has become unusable. Whenever there is a production stoppage, the problem is located, fixed, and restarted at an appropriate point. Production problems are attributed to bad code or patching. The OSS has audit capabilities and that facility is occasionally used.

In the event of an extended system unavailability, all data entry clerks and computer operators, as well as the

other ADP personnel, manually perform the computer's critical processing. All personnel are required to work an extended shift (10 hours) if an extended system unavailability occurs. Each hour of manual critical processing costs the company \$7,500.

The data communications system consists of one communications controller and one modem located in the ADP Building. These are connected by a single, underground line to one modem and four multiplexers (one primary and three secondary) located in an uncontrolled area of the Administration Building. The communications equipment is five years old. As with the ADP equipment, the repairs to the data communications system are accomplished on a 'per incident' basis by a contractor. There is no regular maintenance on the communications system.

f. Administration

Security for the data is considered to be a low priority item, primarily due to budget. Documentation of operating and administrative procedures are located throughout the Center, but not kept up-to-date. The Center works one shift (eight hours) per day and normally generates \$5,000 per hour in revenue.

The system is 'hacker friendly' (e.g., no passwords, no warning screen). It is not difficult to 'crash' the network and enter the operating system, or other

applications. The company relies on software packages from the vendor to keep the system operational, and any enhancement the vendor chooses to put on the system is accepted. Any staff working outside normal hours have access to programming and editing facilities. The staff works on the system unsupervised. The organization does not rely on the communications equipment, therefore, its failure is not likely to result in complete stoppage. The network will continue to function in a degraded mode.

The On-line Pay/Personnel system and Financial/Management information system are processed in the batch mode. All data entry is performed by data entry clerks. Updates to the master Pay/Personnel files are usually backlogged two to three days. All other data entry is often backlogged two weeks. Because of backlog, ten (of 20) data entry clerks and five (of ten) computer operators each work two hours per day (ten hours/week) overtime. As a result, computer operations are now scheduled for ten hours (eight hours plus two hours overtime) daily. All employees receive time-and-a-half for overtime work. Operating expenses (utilities, etc.) incurred from overtime amounts to \$3,000 per hour.

g. Management Philosophy and Concerns

The converted data center was established to meet the immediate and expanding needs of the corporation. In

addition to meeting these needs, a small information technology (IT) group was developed. The group's primary responsibilities include; monitoring technological growth, specialization of contemporary technology, and assisting the users with the significant shifts in the types of applications being automated. During the conversion, top corporate management tasked the IT group with all facets of ADP security. A risk assessment of corporate information systems is required annually. The CERTS DSS was selected to assist in this process. Pairwise comparisons were made of all the criteria in the DSS. For example, credibility was deemed to be more important than any other criteria. The rankings and DSS assigned weights on the evaluated criteria are presented in Table 30.

The IT group is very concerned with output reliability and the merit of desired/required changes. This concern falls within the scope of credibility. When dealing with a data center, one needs to possess a strong sense of flexibility. Data in this environment is volatile and is constantly being altered. In this situation, data sensitivity is primarily based on its integrity requirement and is considered highly sensitive. The management staff is seeking a risk management package or tool that will instill and maintain the confidence of the analyst throughout the entire process. The output of the process must have an obvious relationship to the data provided.

TABLE 30. DATA CENTER

Ranking	Criteria	DSS Assigned Weight
1	Credibility	.354
2	Validity	.240
3	User Interface	.159
4	Feasibility	.104
5	Consistency	.068
6	Completeness	.045
7	Adaptability	.031

The natural feel for the input, process, and output of a method is supported by the amount of information available to the user. This data center has numerous problems with unreliable equipment, software failures, and poor employee performance. These problems may result in a multitude of different risk conditions. The reliability of the package is critical to allow results to be repeated, and therefore, has a direct bearing on the credibility of a process. Table 31 shows the rankings and the DSS assigned weights for the credibility subcriteria.

The validity of a risk management package closely follows the credibility criteria. As the processing method may be done manually or with the current computer configuration, the package must be able to address the scope of the processing status. The tool must be able to provide the scope and detail required by the analyst to be valid.

TABLE 31. CREDIBILITY

Ranking	Subcriteria	DSS Assigned Weight
1	Intuitiveness	.560
2	Reliability	.440

Because of the organization's tremendous dependency on the hardware vendor to solve problems, the relevancy of the results are critical. The desired results should provide categories of solutions rather than specific recommendations. Table 32 presents the rankings and the DSS assigned weights for the validity subcriteria.

User interface is the next concern of the management. The average percentage of turnover in staff per year is 40%. This turnover rate is also reflected in the risk management staff. Therefore, management is searching for a package that does not require the user to grasp all the aspects of the process, but would allow an appreciation of the requirements of the system. Understanding the process contributes to the ease of use attribute. Again, due to such a high turnover rate, a consistent interface must exist that allows the analyst to concentrate on his task rather than on the process itself. The group is seeking a package with well written documentation, on-site training, on-site repair, and 24 hour phone support. Table 33 provides the rankings and the DSS assigned weights for the user interface subcriteria.

The criterion of feasibility is of less concern to management because the availability of the data is accessible both within and external to the organization. The cost of gathering the required data has been determined to be minimal. A conscientious decision to invest the necessary effort and time to accomplish this task has been made. Table 34 depicts the rankings and the DSS assigned weights for the feasibility subcriteria.

The remaining three criteria: consistency, completeness, and adaptability are considered less important than the first four criteria. The IT group at this time prefers to focus on the first four criteria as the major requirement for the system.

TABLE 32. VALIDITY

Ranking	Subcriteria	DSS Assigned Weight
1	Scope	.392
2	Relevancy	.330
3	Practicality	.278

The three remaining criteria were ranked in the order of consistency, completeness, and then adaptability. Due to the less significance of these criteria, all subcriteria within each criteria were determined to be of equal importance. Tables 35, 36, and 37 summarize the

rankings and the DSS assigned weights of the each criteria, respectively.

The CERTS DSS selected LAVA as the best risk management package for the data center scenario. The detailed results are shown in Appendix F, Templates 1 through 3.

TABLE 33. USER INTERFACE

Ranking	Subcriteria	DSS Assigned Weight
1	Understandable	.230
2	Ease of Use	.210
3	Support	.196
4	Simplicity	.188
5	Error Handling	.175

TABLE 34. FEASIBILITY

Ranking	Subcriteria	DSS Assigned Weight
1	Scope	.392
2	Availability	.330
3	Practicality	.278

TABLE 35. CONSISTENCY

Ranking	Subcriteria	DSS Assigned Weight
1	Reliability	.500
1	Consistent Terminology	.500

TABLE 36. COMPLETENESS

Ranking	Subcriteria	DSS Assigned Weight
1	Attributes	.333
1	Elements	.333
1	Scope	.333

TABLE 37. ADAPTABILITY

Ranking	Subcriteria	DSS Assigned Weight
1	Modifiability	.500
1	Portability	.500

As with the previous two case studies, a sensitivity analysis can be performed for the data center. If the IT group determines that the completeness of a package needs more emphasis, then the CERTS DSS would select BDSS as the best risk management tool for the data center. The sensitivity analysis is illustrated in Appendix F, Template 4.

VI. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

1. CERTS Decision Support System

Garrabrants and Ellis developed an approach, CERTS, which would select the best risk management tool for a given organizational situation. While this approach is beneficial to organizations, it is, in its current form, very complex and time consuming to apply. It requires answering an extensive series of questionnaires for each risk management package that an organization is considering. Additionally, extensive calculations are required to synthesize the results of the questionnaires into a suitability index that helps the organization to select the best risk management package. Garrabrants and Ellis' approach also offers no way to weight certain metrics of the questionnaire which are more important to the organization selecting the risk management package.

Combining CERTS with the AHP approach into an automated Decision Support System alleviates many of the above weaknesses. First, it is simple and easy to use. Second, the decision support system does not require the analysts of the organization to become experts in all the risk management packages under consideration. The analysis of the risk management packages with respect to the detailed

subsubcriteria is already completed and incorporated in the decision support system. Third, all calculations are done automatically, thus saving a considerable amount of time and effort.

The CERTS Decision Support System is based on T.L. Saaty's Analytical Hierarchy Process (AHP). Under this approach, the decision of selecting the best risk management package is modeled as a hierarchy. The top level is considered the goal, and the subsequent levels represent the criteria, subcriteria, and subsubcriteria with each succeeding level being a refinement of the higher level. Finally, the leaves of the hierarchy represent the alternatives, which are the risk management packages under consideration. The basis for making the selection is the pairwise comparison of the criteria, subcriteria, and subsubcriteria. In this way, organizations can place more importance on certain criteria, subcriteria, or subsubcriteria which they deem more important for their particular situation. After all pairwise comparisons are made, the decision support system selects the best risk management package for that given situation.

2. Case Studies

The case studies used for applying the CERTS Decision Support System were based on cases that the National Institute of Standards and Technology's Risk Management Laboratory used in testing risk management packages. All aspects of the cases

were based on hypothetical organizations while the management philosophy and concerns were the authors' inferences and conclusions based on the description of each particular case.

These inferences and conclusions were then used to make the pairwise comparisons in the CERTS Decision Support System. Depending on the requirement of each case, the decision support system selected a risk management package to best meet the needs of each organization.

When an organization, through pairwise comparison, establishes the importance of each criteria, subcriteria, or subsubcriteria, the CERTS Decision Support System assigns weights to each criteria and selects the best risk management package for the organization.

As each risk management package has its strengths and weaknesses, and each organization has different requirements, there is no single package that could be designated as the package of choice for all organizations. Since the strengths and weaknesses of each package under consideration are incorporated in the DSS, pairwise comparisons based on the organizations's requirements, will result in selecting the best package for the organization.

B. RECOMMENDATIONS

The CERTS DSS needs to include more risk management packages, at the leaf nodes of the hierarchy, to make the tool beneficial for organizational usage. This study used only

three risk management packages in developing the DSS. There are numerous risk management packages available for organizations, and for the DSS to be effective, these packages need to be analyzed and placed in the hierarchy so that the package selected by the DSS is the best available package.

The criteria, subcriteria, and subsubcriteria of the DSS need to be refined further. The metrics from Garrabrants and Ellis' thesis were modified for this study, but further refinement is necessary to make the DSS a more effective tool.

Validation of the CERTS DSS needs to be accomplished on actual case studies. This study was completed by using hypothetical cases. To determine the effectiveness of the DSS, real life case situations should be used for evaluation.

Elimination of infeasible alternatives should be accomplished before the DSS is used by an organization. For example, an organization wants to spend no more than \$1,000 for the risk management package. The system should screen out those risk management packages costing over \$1,000 and establish the DSS only with alternatives meeting the requirements.

APPENDIX A. SUBSUBCRITERIA OF THE DECISION SUPPORT SYSTEM

TEMPLATE 1.

Consistency Criteria

Subcriteria	Subsubcriteria
Reliability	Reducing the introduction of personal bias
	Reducing the impact of uncertainty
Consistent Terminology	Establishing standard language
	Defining method for the user
	Requesting input in designated units
	Requesting input unambiguously

TEMPLATE 2.

User Interface Hierarchy

Subcriteria	Subsubcriteria
Error Handling	Readily identifying data entry errors
	Facilitating the handling of data entry errors
	Being insensitive to insignificant data accuracy errors
Simplicity	Requiring smaller knowledge base to operate the process
	Mitigating complex relationships for the user
	Defining problem domain
	Not requiring special training to operate
	Not requiring special training to interpret reports
Ease of Use	Having standardized interface
	Differentiating one iteration clearly from others
	Being well structured and logically sequential
	Requested info being relevant
Understandability	Explaining underlying premise
	Premise being comprehensible
	Defining terms unambiguously
	Explaining relationships between phases and iterations
	Identifying decision points clearly
Support	Developer providing support for product
	Providing technical support by phone
	Providing written documentation
	Providing on site training

TEMPLATE 3.

Adaptability Hierarchy

Subcriteria	Subsubcriteria
Portability	Applying across system configurations
	Applying across processing methods
	Applying across different environments
	Applying across all phases of system life cycle
Modifiability	Retaining inputs in original form
	Segmenting calculations by identifiable partitions
	Modifying software package

TEMPLATE 4.

Feasibility Hierarchy

Subcriteria	Subsubcriteria
Availability	Requiring expert opinion for methods internal to the organization
	Required data being internal to the organization
	Collection of data being convenient at the scope desired
Practicality	Allowing input in a variety of forms
	Performing the process by available staff
	Time being available to perform the process
	Obtaining precision economically
Scope	User selecting amount of detail
	Bounding detail at the level desired
	Analyzing all data aspects of the system
	Analyzing procedural aspects of the system
	Analyzing personnel aspects of the system
	Analyzing communication aspects of the system
	Analyzing environment of the system

TEMPLATE 5.

Completeness Hierarchy

Subcriteria	Subsubcriteria
Scope	User selecting amount of detail
	Bounding detail at the level desired
	Analyzing all data aspects of the system
	Analyzing procedural aspects of the system
	Analyzing personnel aspects of the system
	Analyzing communication aspects of the system
	Analyzing environment of the system
Elements	Comprehensively considering assets
	Comprehensively considering threat agents
	Comprehensively considering threat events
	Comprehensively considering safeguards
	Comprehensively considering vulnerabilities
	Considering outcomes
Elements Attributes	Considering asset values
	Considering potency of threat agents
	Considering undesirability of threat events
	Considering effectiveness of safeguards
	Considering severity of outcomes
	Considering probabilities of the occurrence of threat events

TEMPLATE 6.

Validity Hierarchy

Subcriteria	Subsubcriteria
Relevancy	Expressing results in terms of solutions rather than specifics
	Results relating to significant areas of need
	Results fulfilling mandated requirements and regulations
	Output results being qualitative
	Output results being quantitative
Scope	User selecting amount of detail
	Bounding detail at the level desired
	Analyzing all data aspects of the system
	Analyzing procedural aspects of the system
	Analyzing personnel aspects of the system
	Analyzing communication aspects of the system
	Analyzing environment of the system
Practicality	Allowing input in a variety of forms
	Performing the process by available staff
	Time being available to perform the process
	Obtaining precision economically

TEMPLATE 7.

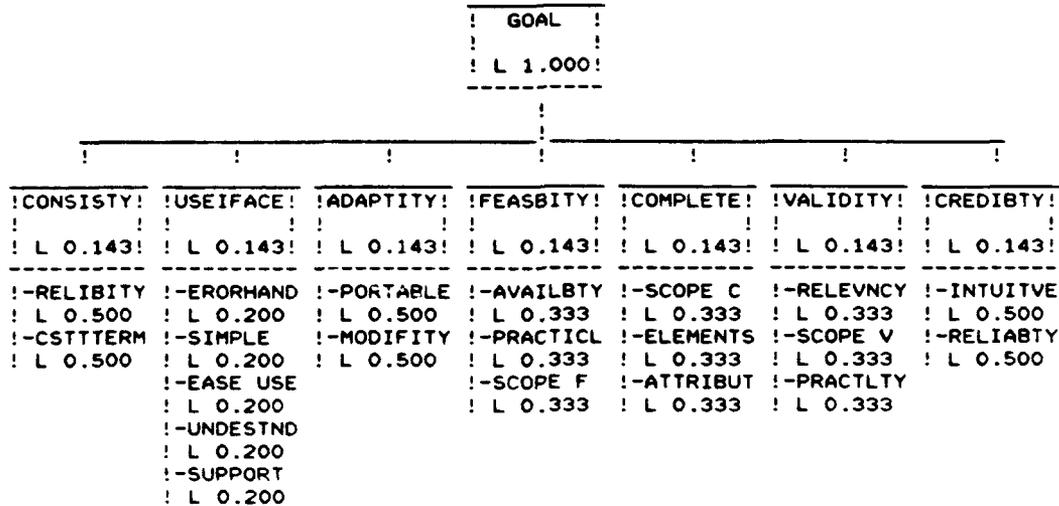
Credibility Hierarchy

Subcriteria	Subsubcriteria
Intuitiveness	Delineating the relationships between the results
	Output being a perceivable relationship with the inputs
	Analyzing all data aspects
	Analyzing procedural aspects
	Analyzing personnel aspects
	Analyzing communication aspects
	Analyzing environment aspects
Reliability	Reducing the introduction of personal bias
	Reducing the impact of uncertainty

APPENDIX B. CERTS DSS HIERARCHY

TEMPLATE 1.

Goal, Criteria, and Subcriteria A COMPARATIVE EVALUATION METHOD FOR RISK MANAGEMENT TOOLS



ADAPTITY --- STRUCTURE OF METHOD CAN BE APPLIED TO VARIOUS SYSTEMS
 ATTRIBUT --- DETERMINATION OF OUTCOMES OR CONSEQUENCES THAT COULD RESULT
 AVAILBTY --- DISTINGUISHES BETWEEN INTERNAL AND EXTERNAL DATA
 COMPLETE --- PROVIDING COMPLETE COVERAGE OF ALL RISK MANAGEMENT PROBLEMS
 CONSISTY --- ABILITY TO DUPLICATE THE RESULTS OF THE PROCESS
 CREDIBTY --- CONCLUSIONS ARE ACCEPTABLE
 CSTTTERM --- UNIFORM SET OF TERMINOLOGY WITHIN THE SYSTEM
 EASE USE --- A PROCESS THAT IS WELL STRUCTURED AND LOGICALLY SEQUENTIAL
 ELEMENTS --- THREE CENTRAL ELEMENTS OPERATE TO DETERMINE THE RISK OF SYSTEM
 ERORHAND --- IDENTIFYING INPUT ERRORS AND RESOLUTION OF THEM
 FEASBITY --- AMOUNT OF EFFORT AND COST TO OBTAIN THE NECESSARY DATA
 INTUITVE --- RESULTS SHOULD INSTILL AND MAINTAIN CONFIDENCE OF ANALYST
 MODIFY --- ASSISTS ANALYSTS IN EXAMINING ALTERNATIVES OR OPTIONS
 PORTABLE --- ABILITY TO APPLY THE PROCESS ACROSS A VARIETY OF SYSTEMS
 PRACTICL --- CONCERNED WITH THE ECONOMICS OF GATHERING THE REQUIRED DATA
 PRACTLTY --- FEASIBILITY OF ACCOMPLISHING DESIRED TASK
 RELEVNCY --- RESULTS ARE MEANINGFUL TO THE SYSTEM
 RELIABTY --- ABILITY TO OBTAIN REPEATABLE RESULTS
 RELIBTY --- OBJECTIVITY OR THE REDUCTION OF SUBJECTIVITY IN THE PROCESS
 SCOPE C --- THE LEVEL OF DETAIL OF ANALYSIS / CONSIDER ALL ASPECTS OF SYSTEMS
 SCOPE F --- INFLUENCES THE ACCEPTABILITY AND USEFULNESS OF A METHOD
 SCOPE V --- DETERMINES THE EXTENT OF THE DETAIL USED BY THE PROCESS
 SIMPLE --- COMPLEXITY OF THE PROCESS IS CONCEALED W/O OBSCURING THE PROCESS
 SUPPORT --- SUPPORT PROVIDED BY THE PROGRAM AND/OR THE DEVELOPER
 UNDESTND --- ABILITY TO COMPREHEND THE UNDERLYING PREMISE THAT SUPPORTS METHOD
 USEIFACE --- THE EFFORT NECESSARY BY OPERATOR TO UNDERSTAND COMPLETE SYSTEM
 VALIDITY --- RESULTS OF THE PROCESS REPRESENT REALITY

L --- LOCAL PRIORITY: PRIORITY RELATIVE TO PARENT

TEMPLATE 2. (continued)

0				

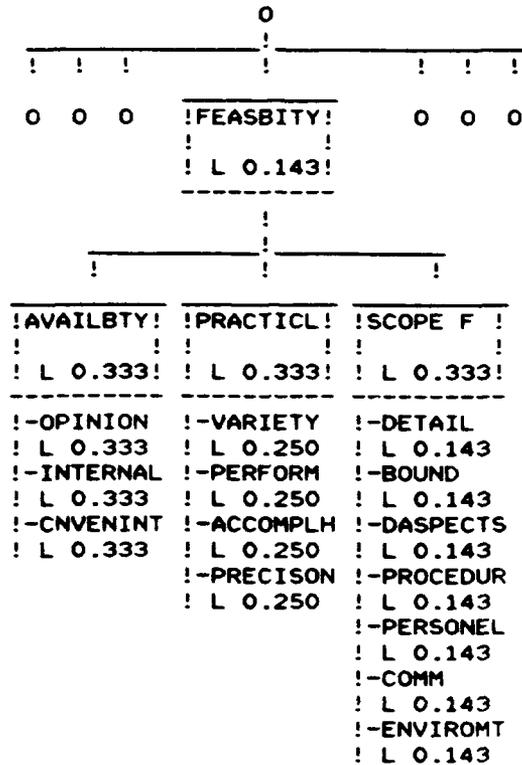
!	!	!	!	!
0	!USEIFACE!	0	0	0
	! L 0.143!			

!	!	!	!	!
!ERORHAND!	!SIMPLE !	!EASE USE!	!UNDESTND!	!SUPPORT !
! L 0.200!				
!-IDENT	!-KNOWBASE	!-INTERFAC	!-PREMISE	!-PRODUCT
! L 0.333	! L 0.200	! L 0.250	! L 0.200	! L 0.250
!-DATAENTY	!-RELATION	!-ITERATIO	!-COMPREHD	!-PHONE
! L 0.333	! L 0.200	! L 0.250	! L 0.200	! L 0.250
!-SENSITVE	!-DOMAIN	!-PROCESS	!-TERMS	!-DOCUMENT
! L 0.333	! L 0.200	! L 0.250	! L 0.200	! L 0.250
	!-TRAINING	!-RELEVANT	!-PHASES	!-SITETRNG
	! L 0.200	! L 0.250	! L 0.200	! L 0.250
	!-RPTTRAIN		!-POINTS	
	! L 0.200		! L 0.200	

- COMPREHD --- COMPREHENDIBLE PREMISE
 DATAENTY --- THE HANDLING OF DATA ENTRY ERRORS
 DOCUMENT --- DEVELOPER PROVIDES WRITTEN DOCUMENTATION OF PROGRAM
 DOMAIN --- PROBLEM DOMAIN WELL DEFINED
 EASE USE --- A PROCESS THAT IS WELL STRUCTURED AND LOGICALLY SEQUENTIAL
 ERORHAND --- IDENTIFYING INPUT ERRORS AND RESOLUTION OF THEM
 IDENT --- DATA ENTRY ERROR IDENTIFICATION
 INTERFAC --- STANDARDIZED INTERFACE
 ITERATIO --- ITERATION CLEARLY DIFFERENTIATED FROM ANOTHER
 KNOWBASE --- SMALLER KNOWLEDGE BASE REQUIRED TO OPERATE THE PROCESS
 PHASES --- R'SHIPS BETWEEN ELEMENTS EXPLAINED BETWEEN PHASES OR ITERATIONS
 PHONE --- TECHNICAL SUPPORT PROVIDED BY PHONE CONVERSATION
 POINTS --- DECISION POINTS CLEARLY IDENTIFIED
 PREMISE --- UNDERLYING PREMISE EXPLAINED
 PROCESS --- PROCESS WELL STRUCTURED AND LOGICALLY SEQUENTIAL
 PRODUCT --- DEVELOPER PROVIDES SUPPORT FOR HIS PRODUCT/PROGRAM
 RELATION --- COMPLEX RELATIONSHIPS MITIGATED FOR THE USER
 RELEVANT --- INFORMATION REQUESTED OF THE USER RELEVANT
 RPTTRAIN --- TRAINING TO INTERPRET REPORTS
 SENSITVE --- INSENSITIVE TO INSIGNIFICANT DATA ACCURACY ERRORS
 SIMPLE --- COMPLEXITY OF THE PROCESS IS CONCEALED W/O OBSCURING THE PROCESS
 SITETRNG --- DEVELOPER PROVIDES TRAINING ON SITE
 SUPPORT --- SUPPORT PROVIDED BY THE PROGRAM AND/OR THE DEVELOPER
 TERMS --- TERMS UNAMBIGUOUSLY DEFINED
 TRAINING --- SPECIAL TRAINING REQUIRED TO OPERATE/UNDERSTAND PROGRAM
 UNDESTND --- ABILITY TO COMPREHEND THE UNDERLYING PREMISE THAT SUPPORTS METHOD
 USEIFACE --- THE EFFORT NECESSARY BY OPERATOR TO UNDERSTAND COMPLETE SYSTEM

 L --- LOCAL PRIORITY: PRIORITY RELATIVE TO PARENT

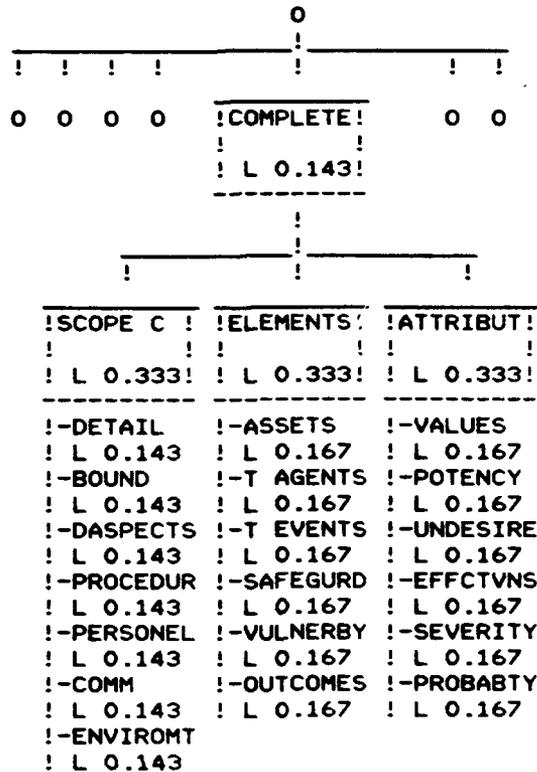
TEMPLATE 2. (continued)



- ACCOMPLH --- TIME IS AVAILABLE TO PERFORM THE PROCESS
- AVAILBTY --- DISTINGUISHES BETWEEN INTERNAL AND EXTERNAL DATA
- BOUND --- METHOD BOUNDS THE DETAIL AT THE LEVEL DESIRED
- CNVENINT --- DATA COLLECTION CONVENIENT AT THE SCOPE DESIRED
- COMM --- ALL COMMUNICATIONS ASPECTS OF THE SYSTEMS ARE ANALYZED
- DASPECTS --- ALL DATA ASPECTS OF THE SYSTEM ARE ANALYZED
- DETAIL --- AMOUNT OF DETAIL USER SELECTABLE
- ENVIROMT --- THE ENVIRONMENT THAT THE SYSTEM RESIDES IN IS ANALYZED
- FEASBITY --- AMOUNT OF EFFORT AND COST TO OBTAIN THE NECESSARY DATA
- INTERNAL --- ALL DATA REQUIRED IS INTERNAL TO THE ORGANIZATION
- OPINION --- EXPERT OPINION REQUIRED FOR THE METHODS INTERNAL TO ORGANIZATION
- PERFORM --- AVAILABLE STAFF PERFORMS THE PROCESS
- PERSONEL --- ALL PERSONNEL ASPECTS OF THE SYSTEM ARE ANALYZED
- PRACTICL --- CONCERNED WITH THE ECONOMICS OF GATHERING THE REQUIRED DATA
- PRECISON --- PRECISION CAN BE OBTAINED ECONOMICALLY
- PROCEDUR --- THE PROCEDURAL ASPECTS OF THE SYSTEM ARE ANALYZED
- SCOPE F --- INFLUENCES THE ACCEPTABILITY AND USEFULNESS OF A METHOD
- VARIETY --- ALLOWS INPUT DATA IN A VARIETY OF FORMS

- L --- LOCAL PRIORITY: PRIORITY RELATIVE TO PARENT

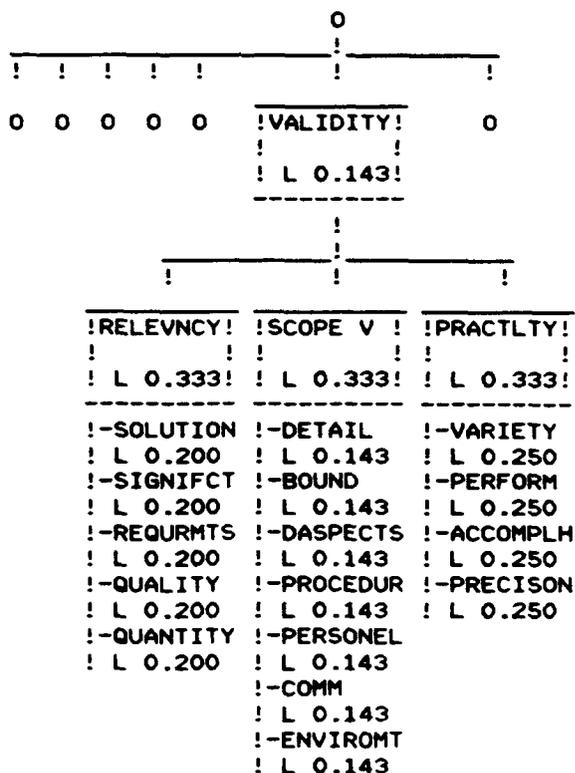
TEMPLATE 2. (continued)



- ASSETS ---- COMPREHENSIVELY CONSIDER ASSETS
- ATTRIBUT ---- DETERMINATION OF OUTCOMES OR CONSEQUENCES THAT COULD RESULT
- BOUND ---- METHOD BOUNDS THE DETAIL AT THE LEVEL DESIRED
- COMM ---- ALL COMMUNICATIONS ASPECTS OF THE SYSTEMS ARE ANALYZED
- COMPLETE ---- PROVIDING COMPLETE COVERAGE OF ALL RISK MANAGEMENT PROBLEMS
- DASPECTS ---- ALL DATA ASPECTS OF THE SYSTEM ARE ANALYZED
- DETAIL ---- AMOUNT OF DETAIL USER SELECTABLE
- EFFCTVNS ---- SAFEGUARD EFFECTIVENESS IS CONSIDERED
- ELEMENTS ---- THREE CENTRAL ELEMENTS OPERATE TO DETERMINE THE RISK OF SYSTEM
- ENVIROMT ---- THE ENVIRONMENT THAT THE SYSTEM RESIDES IN IS ANALYZED
- OUTCOMES ---- CONSIDER OUTCOMES
- PERSONEL ---- ALL PERSONNEL ASPECTS OF THE SYSTEM ARE ANALYZED
- POTENCY ---- POTENCY OF A THREAT AGENT IS CONSIDERED
- PROBABTY ---- PROBABILITY OF THE OCCURENCE OF A THREAT EVENT IS CONSIDERED
- PROCEDUR ---- THE PROCEDURAL ASPECTS OF THE SYSTEM ARE ANALYZED
- SAFEGURD ---- COMPREHENSIVELY CONSIDER SAFEGUARDS
- SCOPE C ---- THE LEVEL OF DETAIL OF ANALYSIS / CONSIDER ALL ASPECTS OF SYSTEMS
- SEVERITY ---- SEVERITY OF OUTCOME IS CONSIDERED
- T AGENTS ---- COMPREHENSIVELY CONSIDER THREAT AGENTS
- T EVENTS ---- COMPREHENSIVELY CONSIDER THREAT EVENTS
- UNDESIRE ---- UNDESIRABILITY OF A THREAT EVENT IS CONSIDERED
- VALUES ---- ASSET VALUES CONSIDERED
- VULNERBY ---- COMPREHENSIVELY CONSIDER VULNERABILITIES

- L ---- LOCAL PRIORITY: PRIORITY RELATIVE TO PARENT

TEMPLATE 2. (continued)



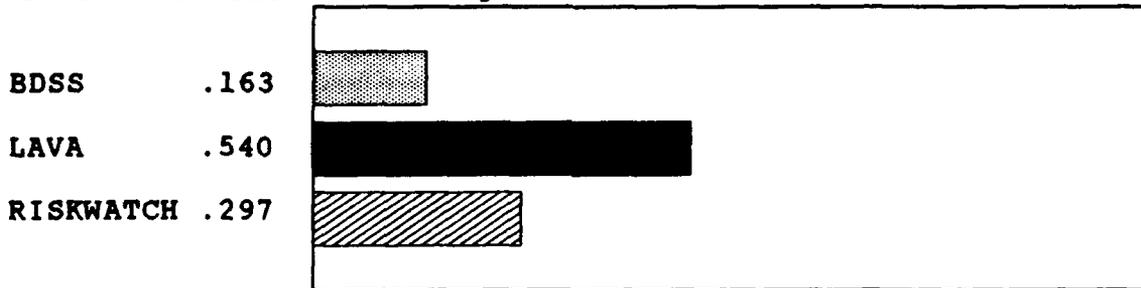
- ACCOMPLH --- TIME IS AVAILABLE TO PERFORM THE PROCESS
- BOUND --- METHOD BOUNDS THE DETAIL AT THE LEVEL DESIRED
- COMM --- ALL COMMUNICATIONS ASPECTS OF THE SYSTEMS ARE ANALYZED
- DASPECTS --- ALL DATA ASPECTS OF THE SYSTEM ARE ANALYZED
- DETAIL --- AMOUNT OF DETAIL USER SELECTABLE
- ENVIROMT --- THE ENVIRONMENT THAT THE SYSTEM RESIDES IN IS ANALYZED
- PERFORM --- AVAILABLE STAFF PERFORMS THE PROCESS
- PERSONEL --- ALL PERSONNEL ASPECTS OF THE SYSTEM ARE ANALYZED
- PRACTLTY --- FEASIBILITY OF ACCOMPLISHING DESIRED TASK
- PRECISON --- PRECISION CAN BE OBTAINED ECONOMICALLY
- PROCEDUR --- THE PROCEDURAL ASPECTS OF THE SYSTEM ARE ANALYZED
- QUALITY --- DESIRED OUTPUT RESULTS ARE QUALITATIVE
- QUANTITY --- DESIRED OUTPUT RESULTS ARE QUANTIATIVE
- RELEVNCY --- RESULTS ARE MEANINGFUL TO THE SYSTEM
- REQRMTS --- FULFILLS MANDATED REQUIREMENTS OR REGULATIONS
- SCOPE V --- DETERMINES THE EXTENT OF THE DETAIL USED BY THE PROCESS
- SIGNIFCT --- RESULTS RELATE TO SIGNIFICANT AREAS OF NEED
- SOLUTION --- RESULTS ARE EXPRESSED IN TERMS OF SOLUTIONS RATHER THAN SPECIFICS
- VALIDITY --- RESULTS OF THE PROCESS REPRESENT REALITY
- VARIETY --- ALLOWS INPUT DATA IN A VARIETY OF FORMS

- L --- LOCAL PRIORITY: PRIORITY RELATIVE TO PARENT

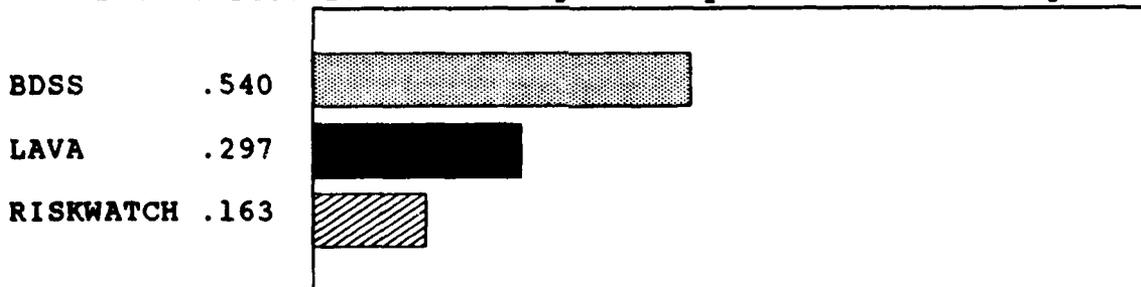
APPENDIX C. DECISION SUPPORT SYSTEM ASSIGNED WEIGHTS FOR ALTERNATIVES

TEMPLATE 1.

Criteria: Consistency
Subcriteria: Reliability
Subsubcriteria: Reducing the Introduction of Personal Bias

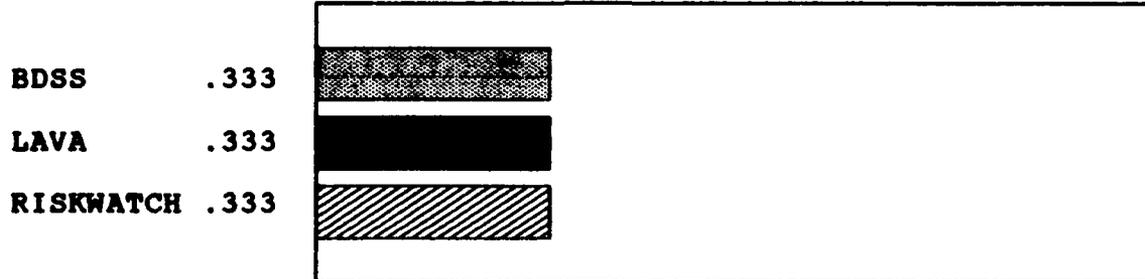


Subsubcriteria: Reducing the Impact of Uncertainty

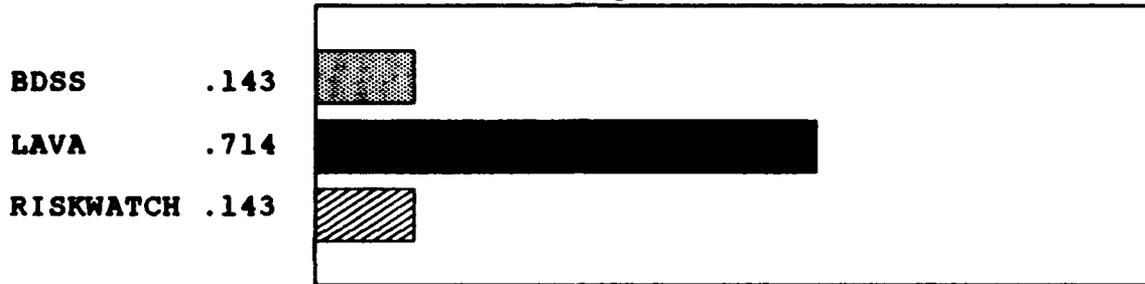


TEMPLATE 2.

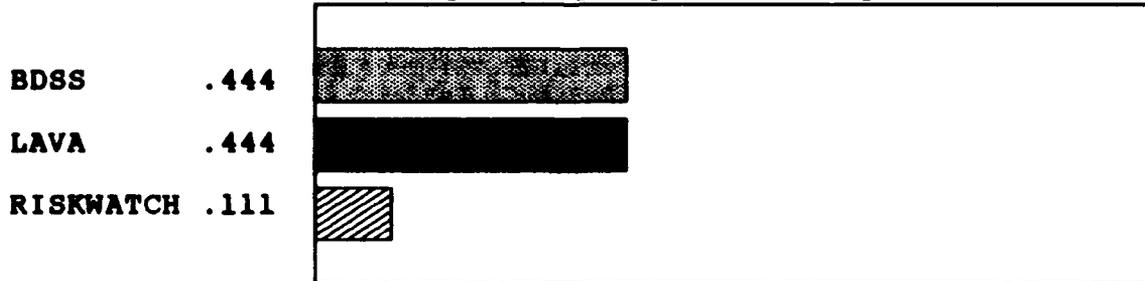
Criteria: Consistency
Subcriteria: Consistent Terminology
Subsubcriteria: Establishing Standard Language



Subsubcriteria: Defining Method for the User



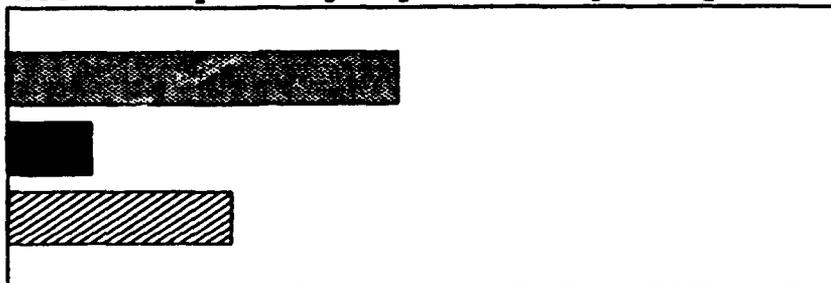
Subsubcriteria: Requesting Input in Designated Units



TEMPLATE 2. (continued)

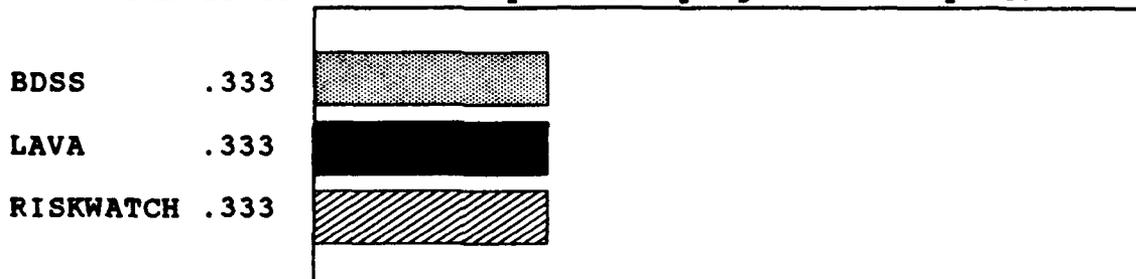
Subsubcriteria: Requesting Input Unambiguously

BDSS .558
LAVA .122
RISKWATCH .320

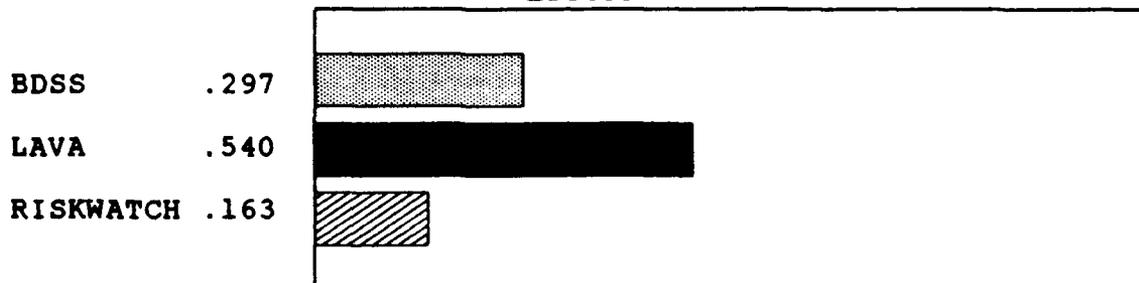


TEMPLATE 3.

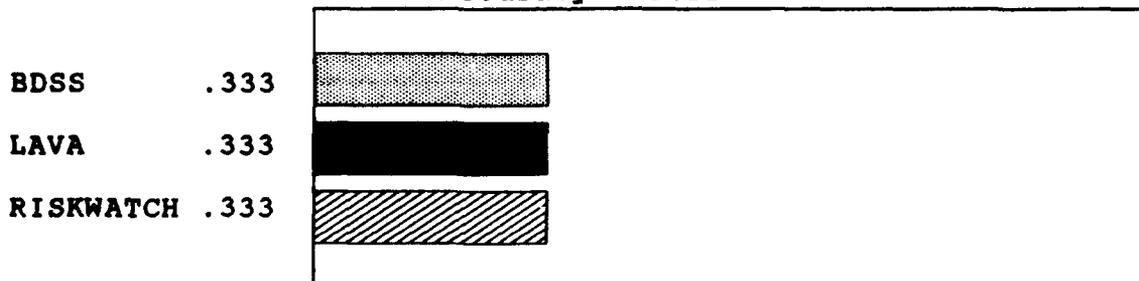
Criteria: User Interface
Subcriteria: Error Handling
Subsubcriteria: Readily Identifying Data Entry Errors



Subsubcriteria: Facilitating the Handling of Data Entry Errors



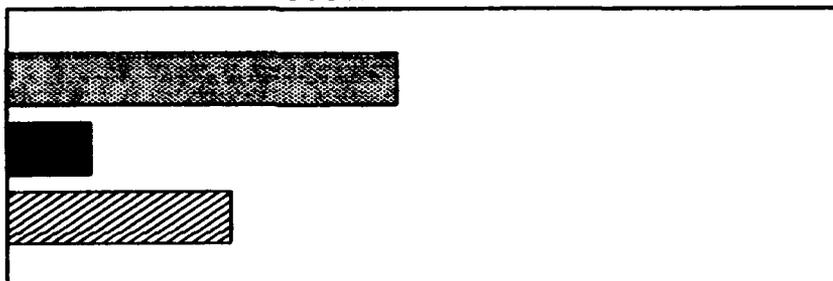
Subsubcriteria: Being Insensitive to Insignificant Data Accuracy Errors



TEMPLATE 4.

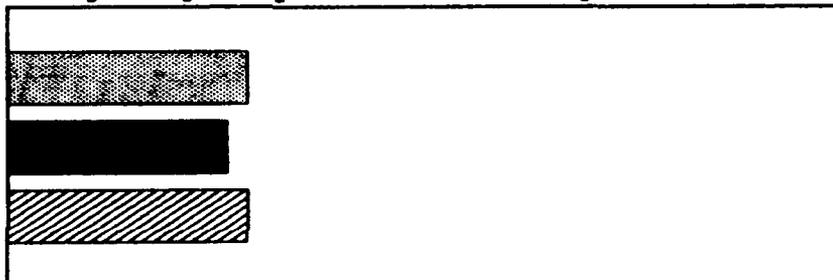
Criteria: User Interface
Subcriteria: Simplicity
Subsubcriteria: Requiring Smaller Knowledge Base to Operate the Process

BDSS .558
LAVA .122
RISKWATCH .320



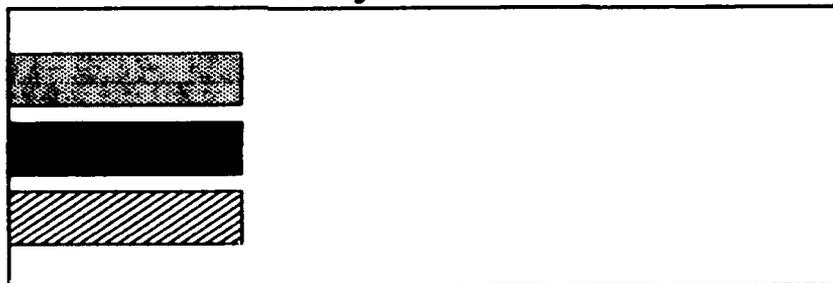
Subsubcriteria: Mitigating Complex Relationships for the User

BDSS .344
LAVA .313
RISKWATCH .344



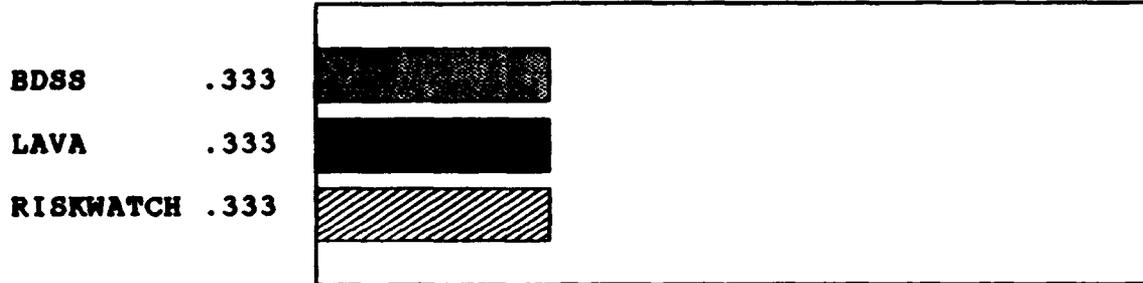
Subsubcriteria: Defining Problem Domain

BDSS .333
LAVA .333
RISKWATCH .333

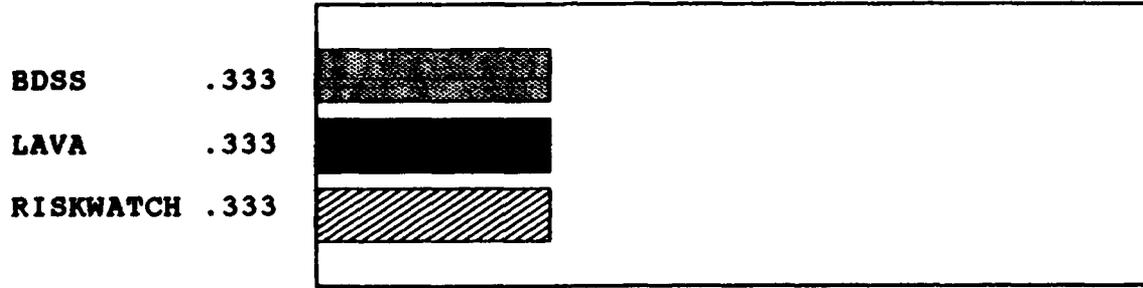


TEMPLATE 4. (continued)

Subsubcriteria: Not Requiring Special Training to Operate

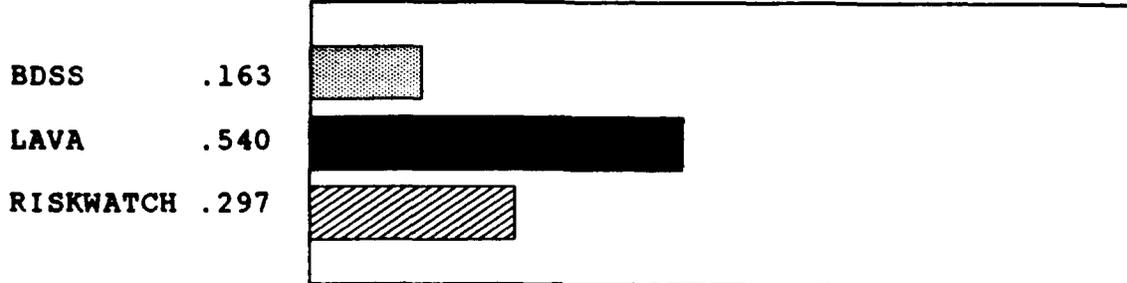


Subsubcriteria: Not Requiring Special Training to Interpret Reports

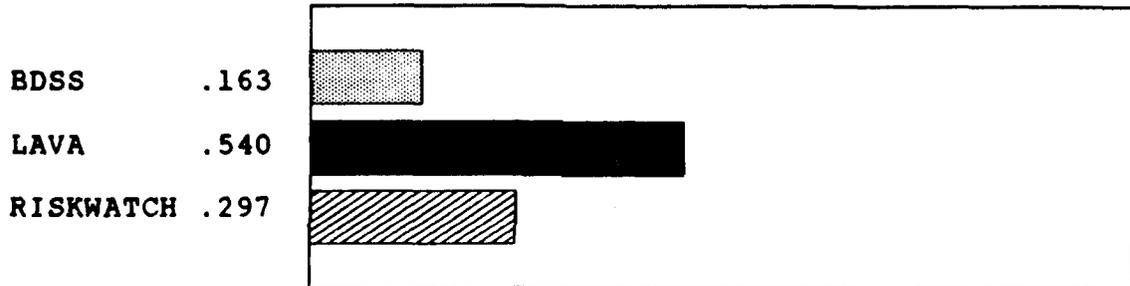


TEMPLATE 5.

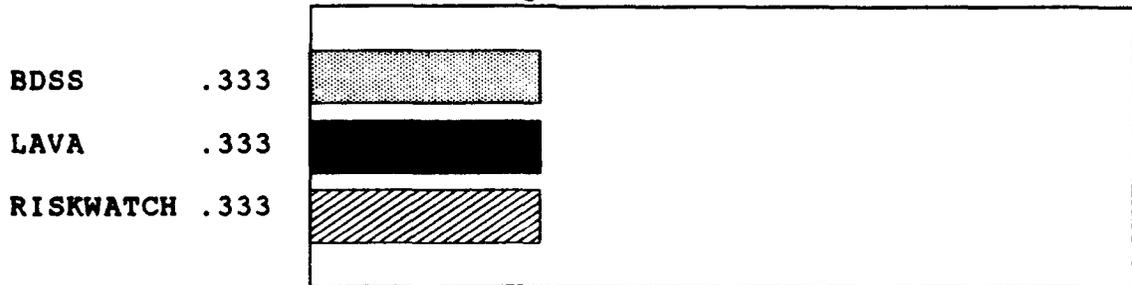
Criteria: User Interface
Subcriteria: Ease of Use
Subsubcriteria: Having Standardized Interface



Subsubcriteria: Differentiating One Iteration Clearly From Others

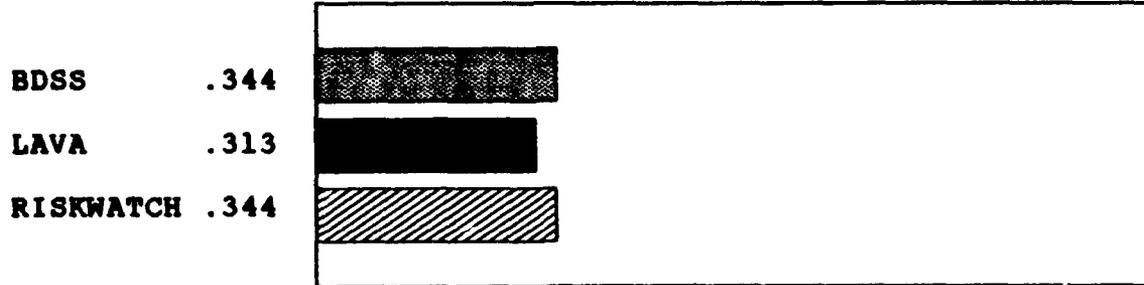


Subsubcriteria: Being Well Structured and Logically Sequential



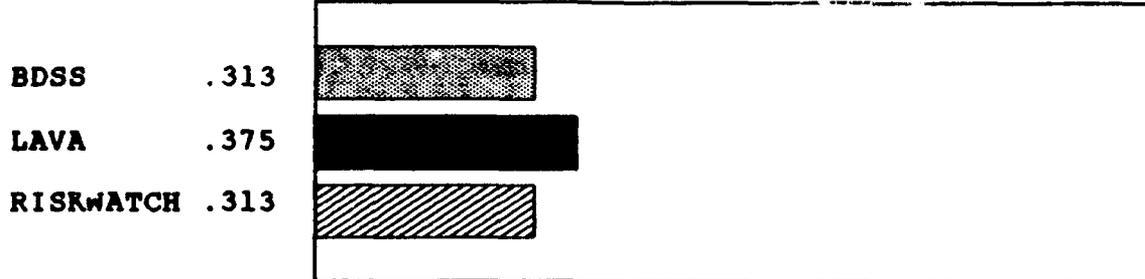
TEMPLATE 5. (continued)

Subsubcriteria: Requested Info Being Relevant

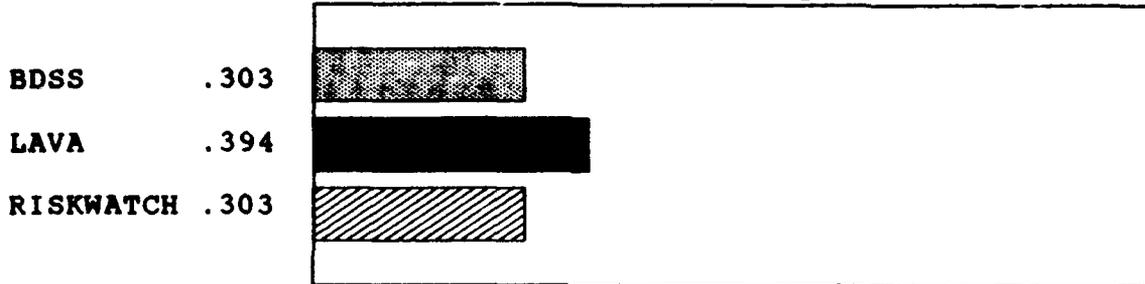


TEMPLATE 6.

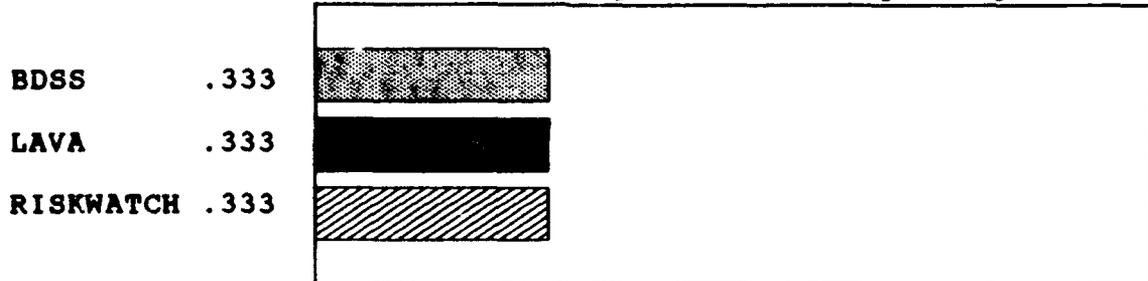
Criteria: User Interface
Subcriteria: Understandability
Subsubcriteria: Explaining Underlying Premise



Subsubcriteria: Premise Being Comprehensible

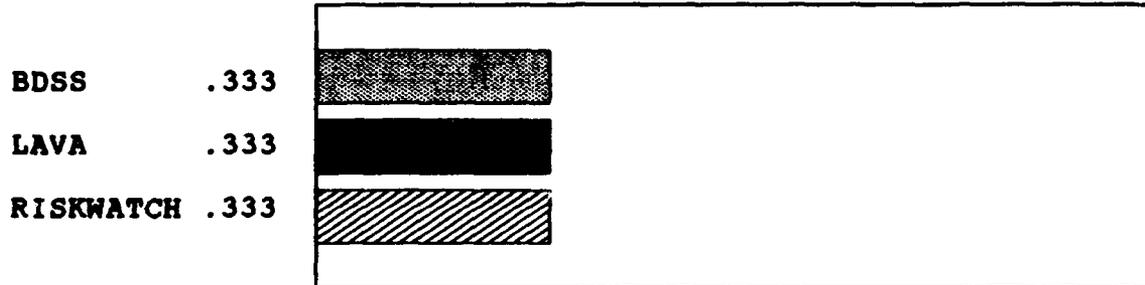


Subsubcriteria: Defining Terms Unambiguously

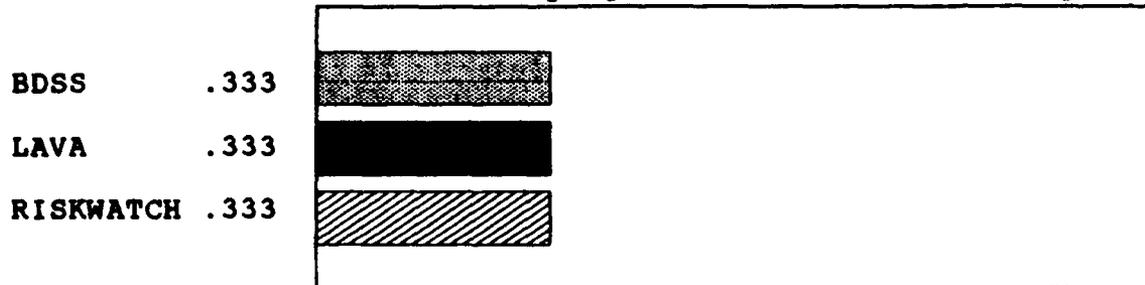


TEMPLATE 6. (continued)

Subsubcriteria: Explaining Relationships Between Phases and Iterations

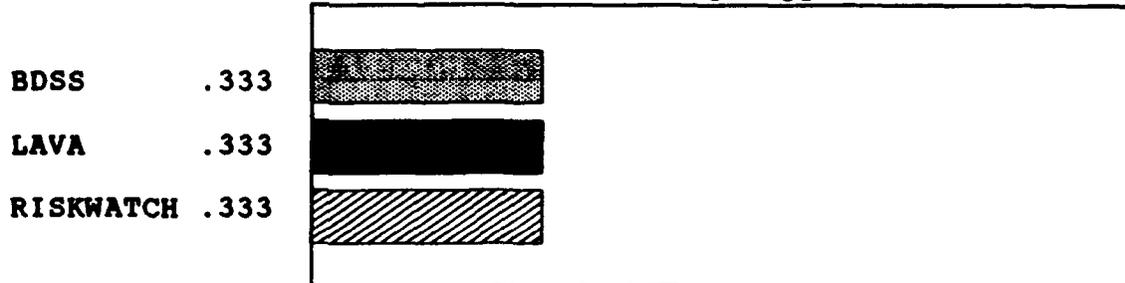


Subsubcriteria: Identifying Decision Points Clearly

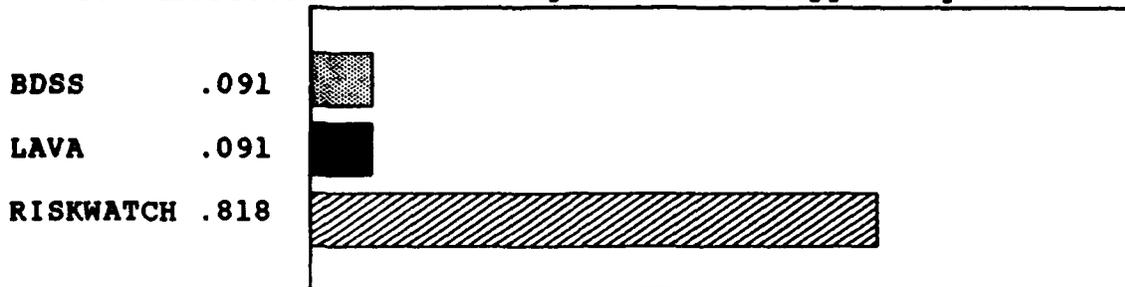


TEMPLATE 7.

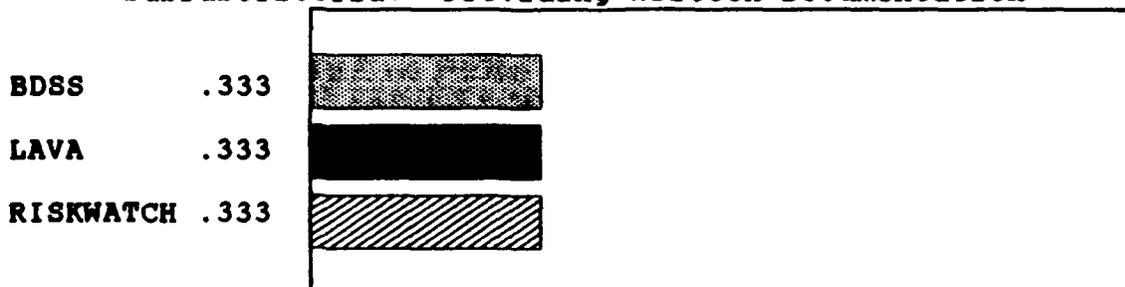
Criteria: User Interface
Subcriteria: Support
Subsubcriteria: Developer Providing Support for Product



Subsubcriteria: Providing Technical Support by Phone

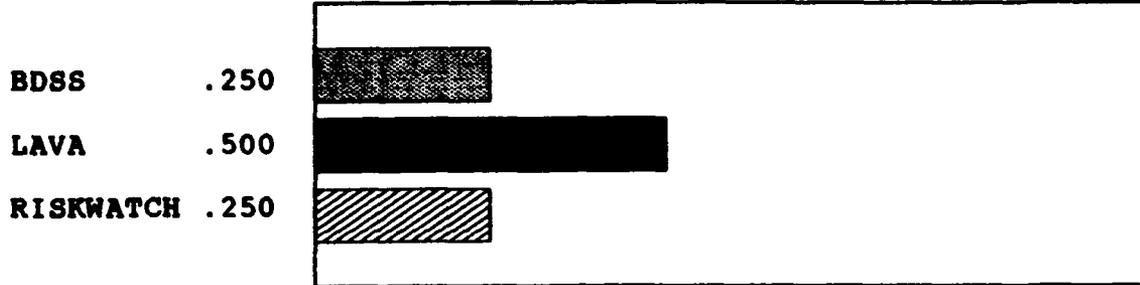


Subsubcriteria: Providing Written Documentation



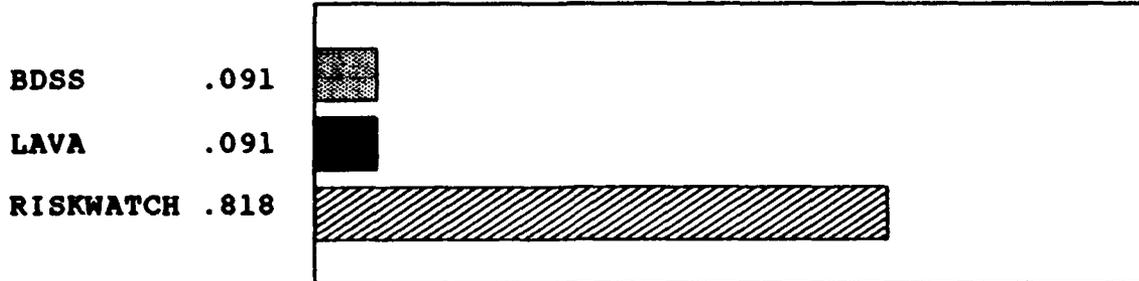
TEMPLATE 7. (continued)

Subsubcriteria: Providing On Site Training

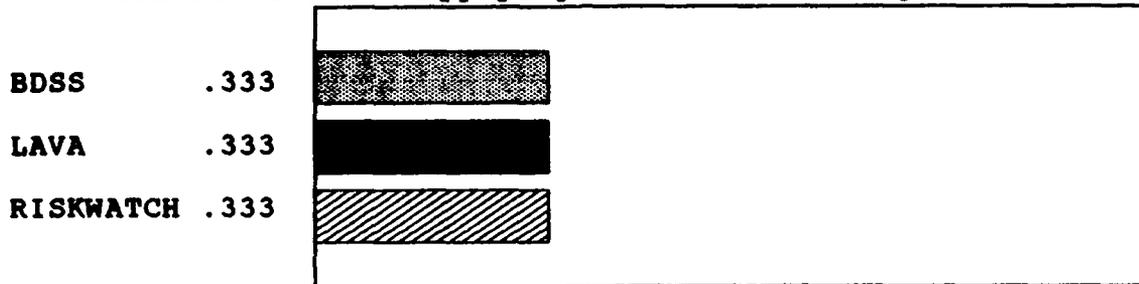


TEMPLATE 8.

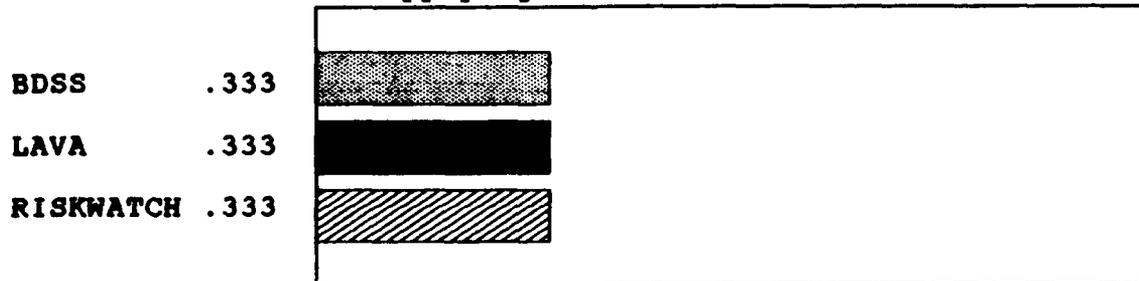
Criteria: Adaptability
Subcriteria: Portability
Subsubcriteria: Applying Across System Configurations



Subsubcriteria: Applying Across Processing Methods

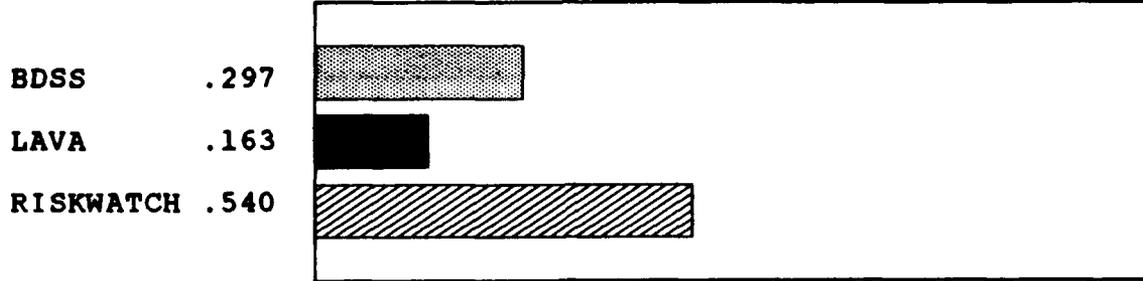


Subsubcriteria: Applying Across Different Environments



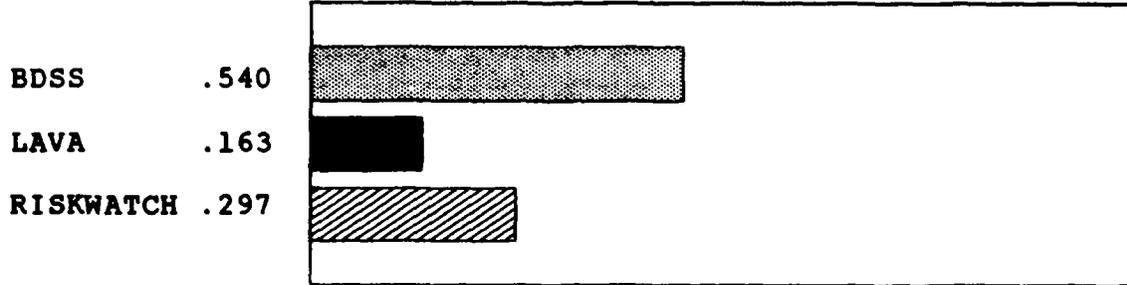
TEMPLATE 8. (continued)

Subsubcriteria: Applying Across All Phases of System Life Cycle

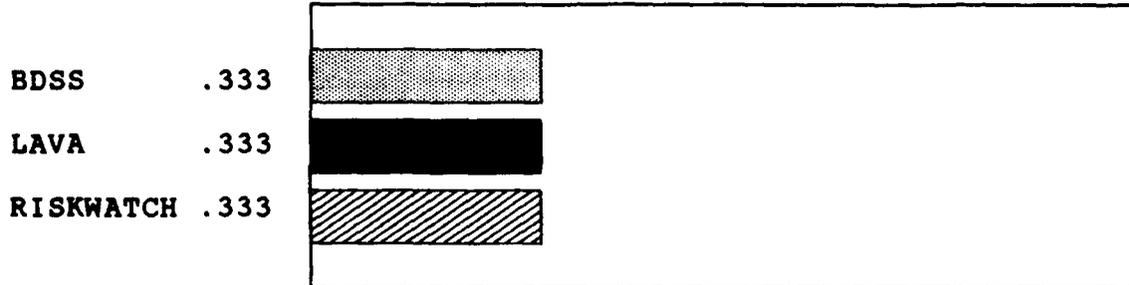


TEMPLATE 9.

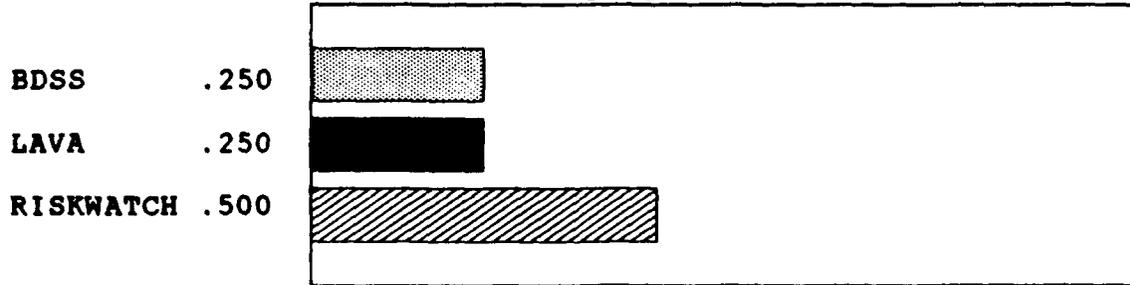
Criteria: Adaptability
Subcriteria: Modifiability
Subsubcriteria: Retaining Inputs in Original Form



Subsubcriteria: Segmenting Calculations by Identifiable Partitions



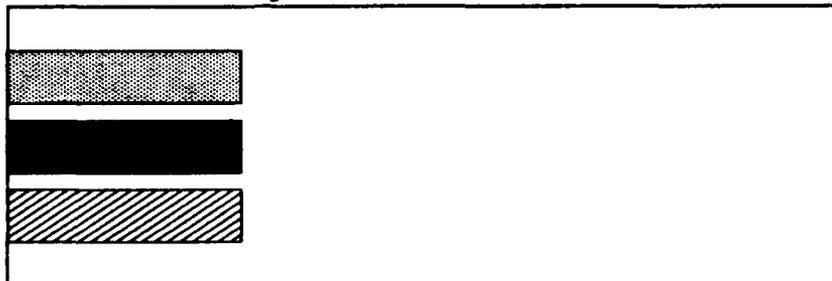
Subsubcriteria: Modifying Software Package



TEMPLATE 10.

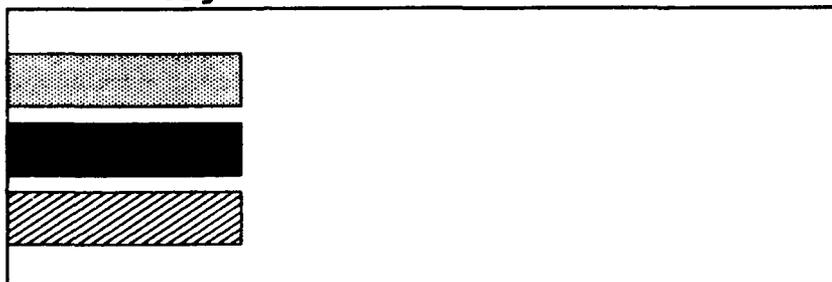
Criteria: Feasibility
Subcriteria: Availability
Subsubcriteria: Requiring Expert Opinion for Methods Internal to the Organization

BDSS .333
LAVA .333
RISKWATCH .333



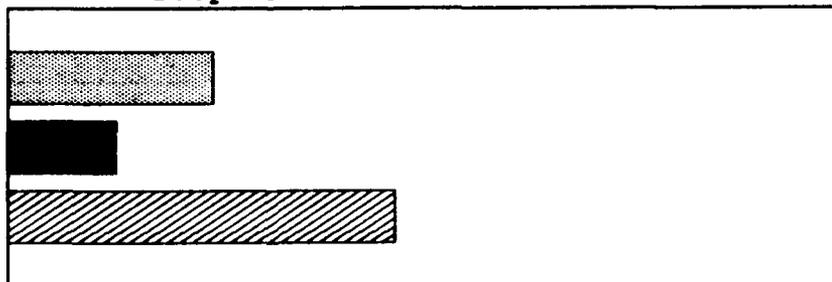
Subsubcriteria: Required Data Being Internal to the Organization

BDSS .333
LAVA .333
RISKWATCH .333



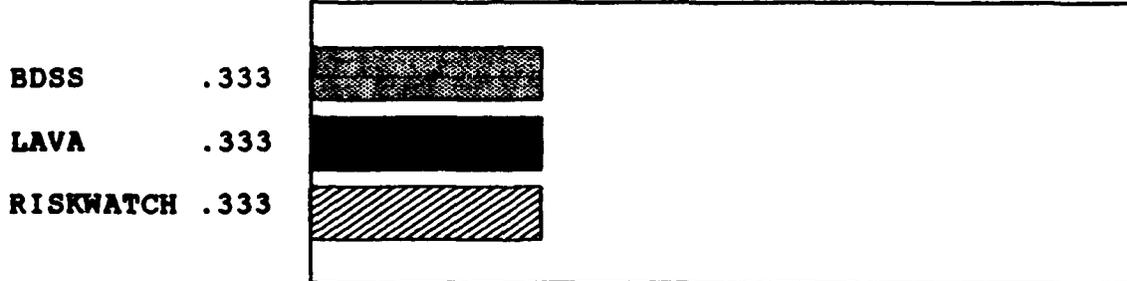
Subsubcriteria: Collection of Data Being Convenient at the Scope Desired

BDSS .293
LAVA .155
RISKWATCH .552

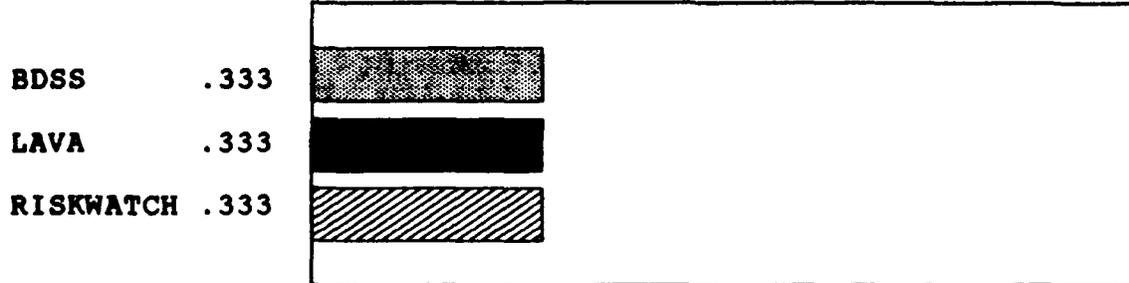


TEMPLATE 11.

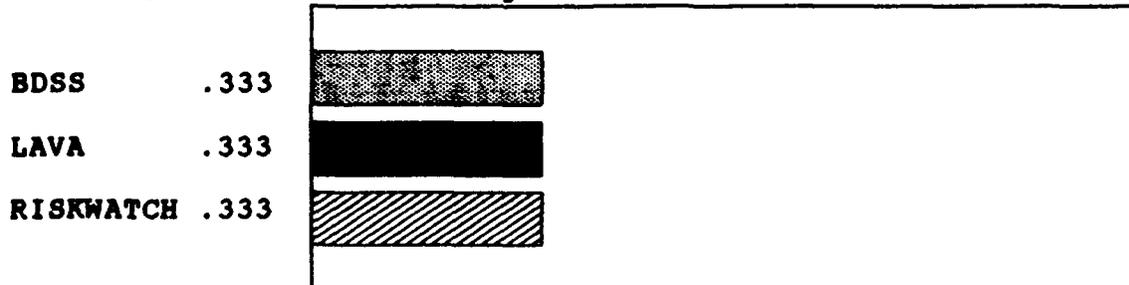
Criteria: Feasibility
Subcriteria: Practicality
Subsubcriteria: Allowing Input in a Variety of Forms



Subsubcriteria: Performing the Process by Available Staff



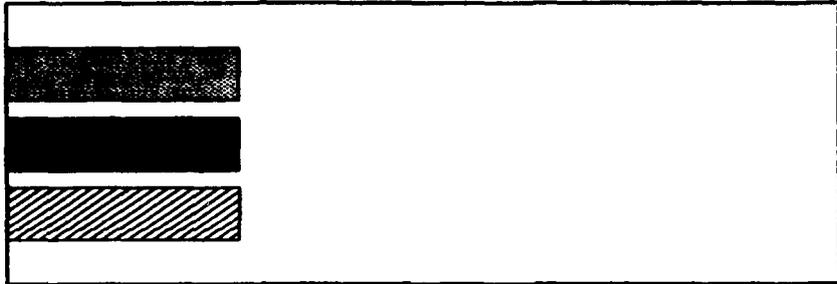
Subsubcriteria: Time Being Available to Perform the Process



TEMPLATE 11. (continued)

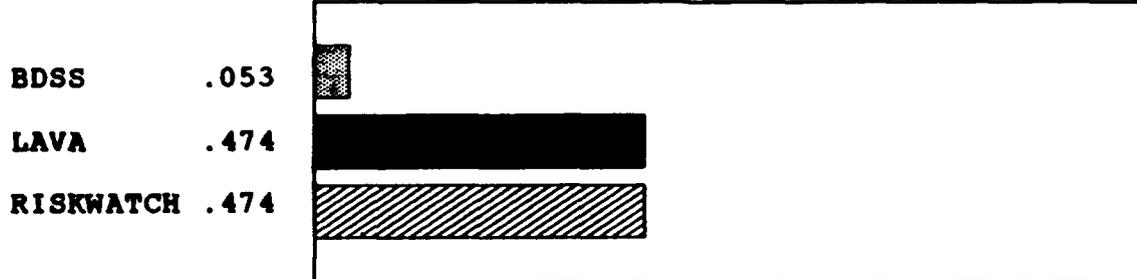
Subsubcriteria: Obtaining Precision Economically

BDSS .333
LAVA .333
RISKWATCH .333

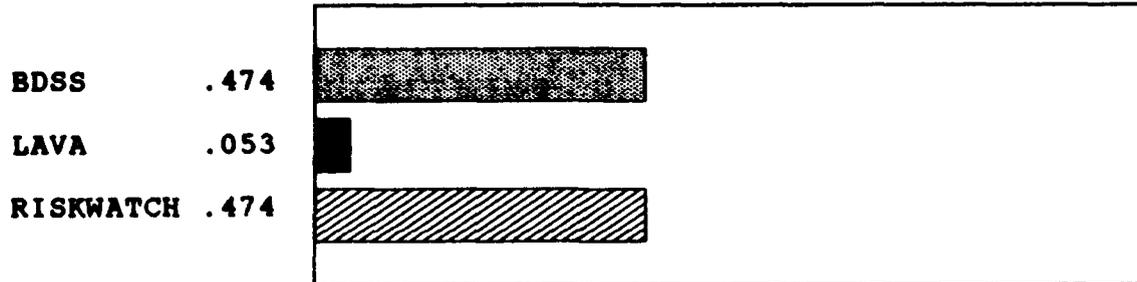


TEMPLATE 12.

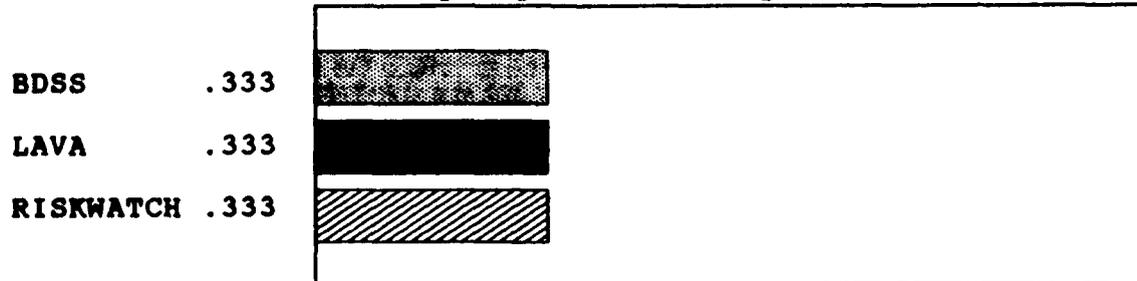
Criteria: Feasibility
Subcriteria: Scope
Subsubcriteria: User Selecting Amount of Detail



Subsubcriteria: Bounding Detail at the Level Desired



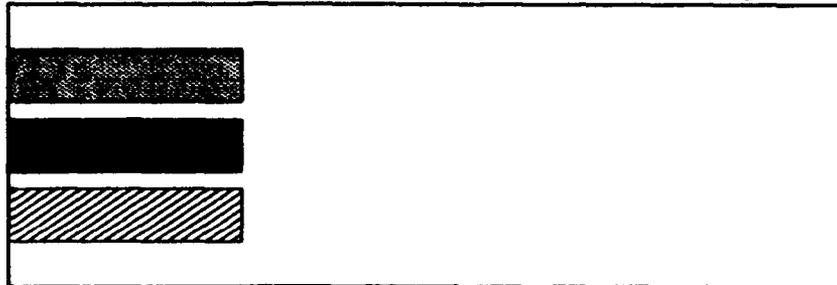
Subsubcriteria: Analyzing All Data Aspects of the System



TEMPLATE 12. (continued)

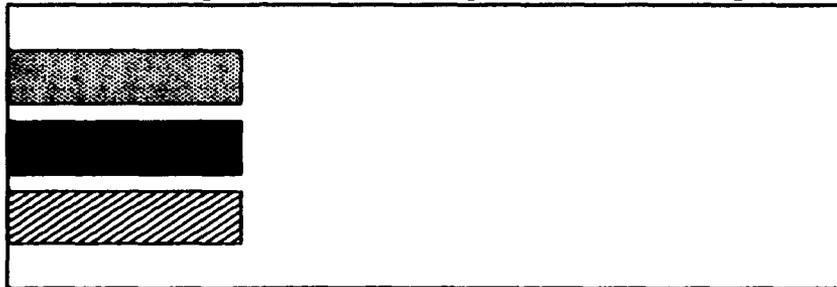
Subsubcriteria: Analyzing Procedural Aspects of the System

BDSS .333
LAVA .333
RISKWATCH .333



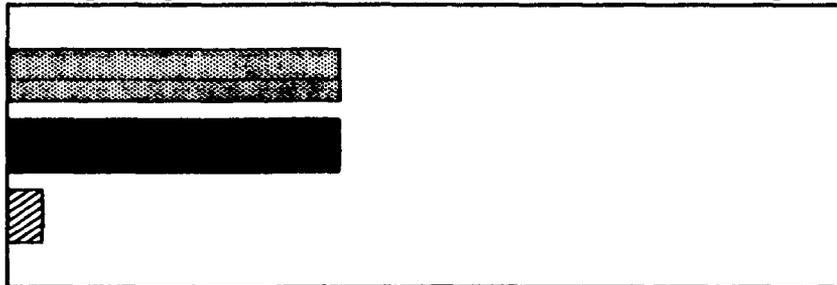
Subsubcriteria: Analyzing Personnel Aspects of the System

BDSS .333
LAVA .333
RISKWATCH .333



Subsubcriteria: Analyzing Communication Aspects of the System

BDSS .474
LAVA .474
RISKWATCH .053



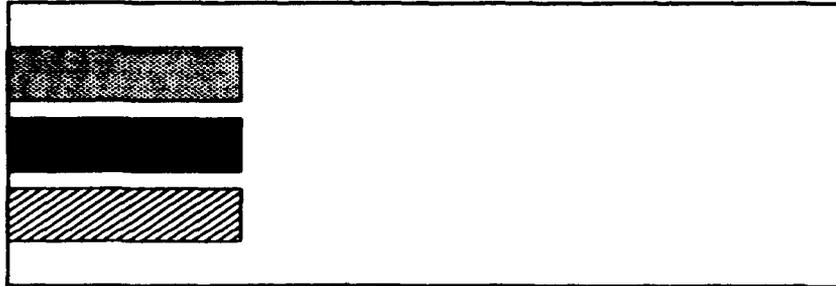
TEMPLATE 12. (continued)

Subsubcriteria: Analyzing Environment of the System

BDSS .333

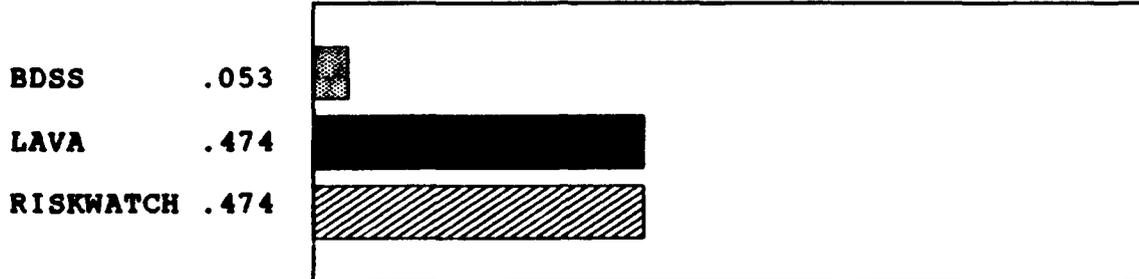
LAVA .333

RISKWATCH .333

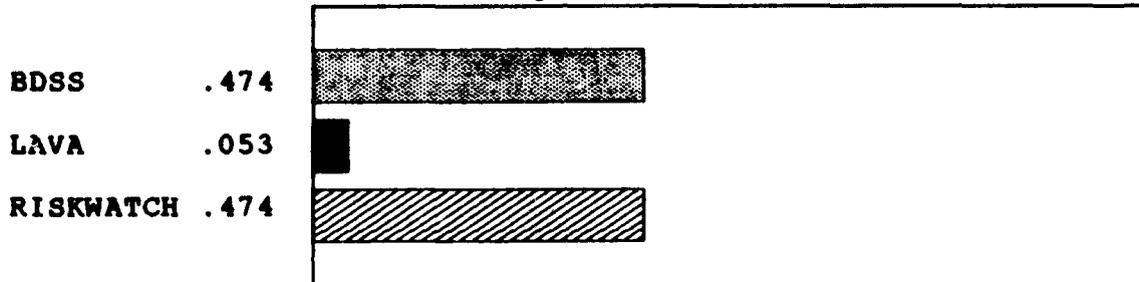


TEMPLATE 13.

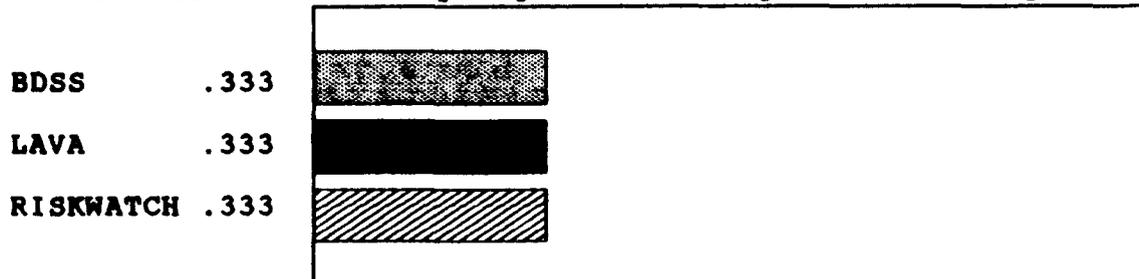
Criteria: Completeness
Subcriteria: Scope
Subsubcriteria: User Selecting Amount of Detail



Subsubcriteria: Bounding Detail at the Level Desired



Subsubcriteria: Analyzing All Data Aspects of the System



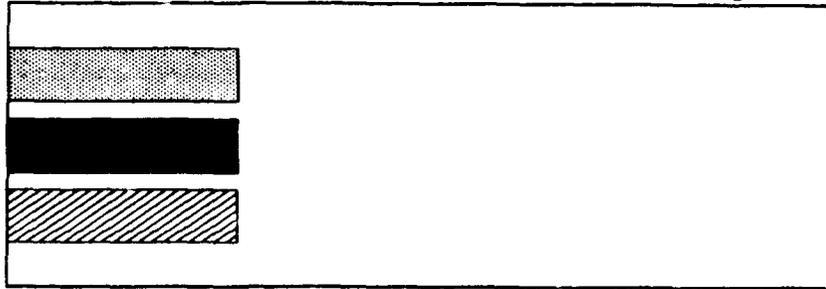
TEMPLATE 13. (continued)

Subsubcriteria: Analyzing Procedural Aspects of the System

BDSS .333

LAVA .333

RISKWATCH .333

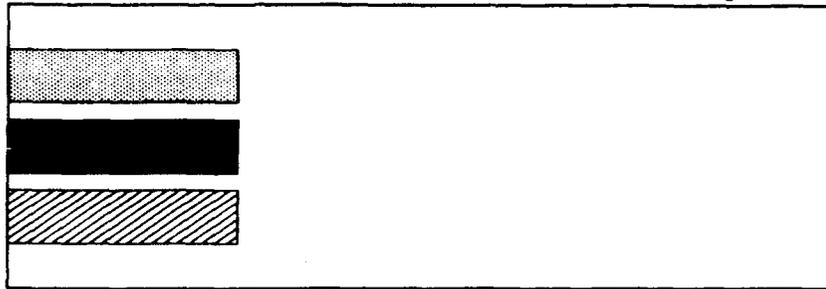


Subsubcriteria: Analyzing Personnel Aspects of the System

BDSS .333

LAVA .333

RISKWATCH .333

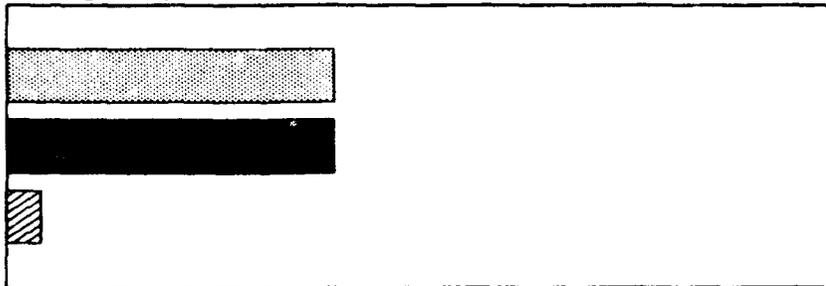


Subsubcriteria: Analyzing Communication Aspects of the System

BDSS .474

LAVA .474

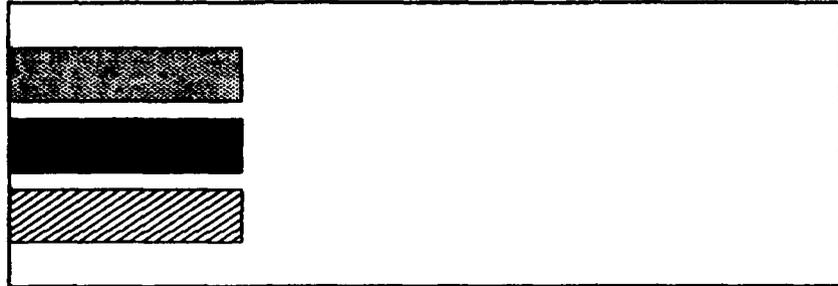
RISKWATCH .053



TEMPLATE 13. (continued)

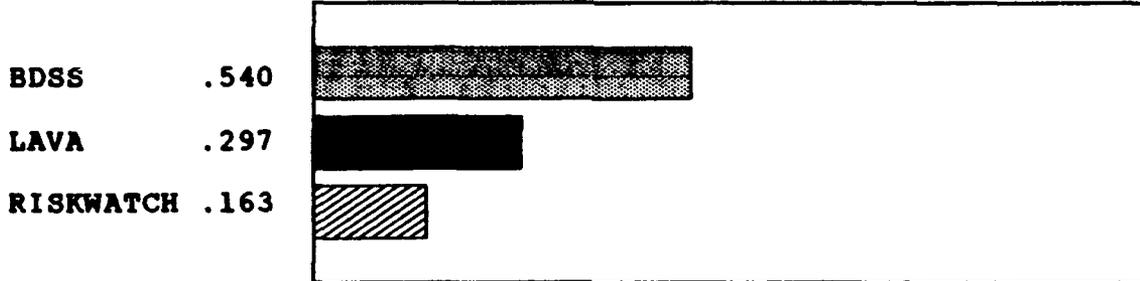
Subsubcriteria: Analyzing Environment of the System

BDSS .333
LAVA .333
RISKWATCH .333

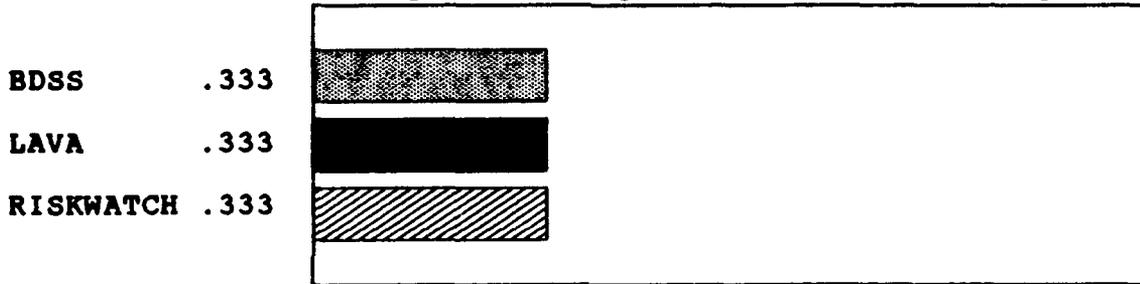


TEMPLATE 14.

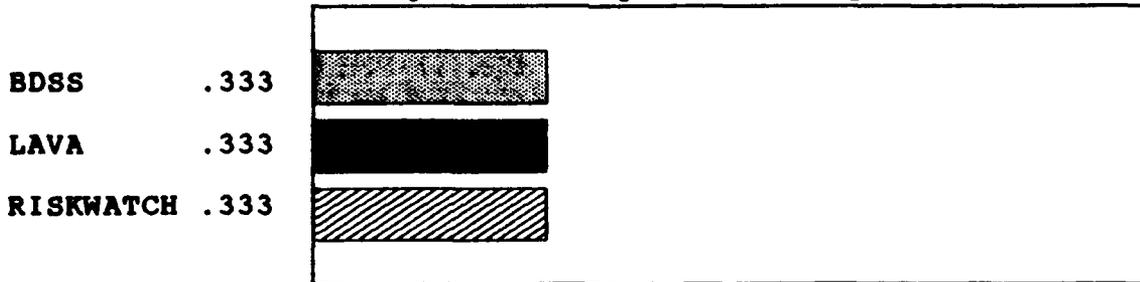
Criteria: Completeness
Subcriteria: Elements
Subsubcriteria: Comprehensively Considering Assets



Subsubcriteria: Comprehensively Considering Threat Agents

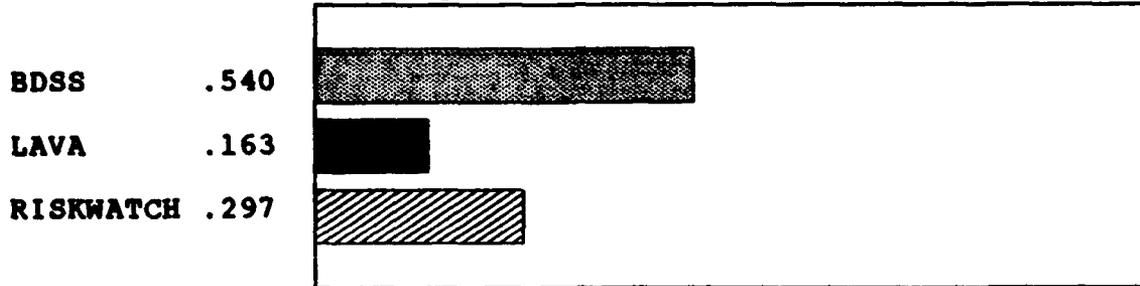


Subsubcriteria: Comprehensively Considering Threat Events

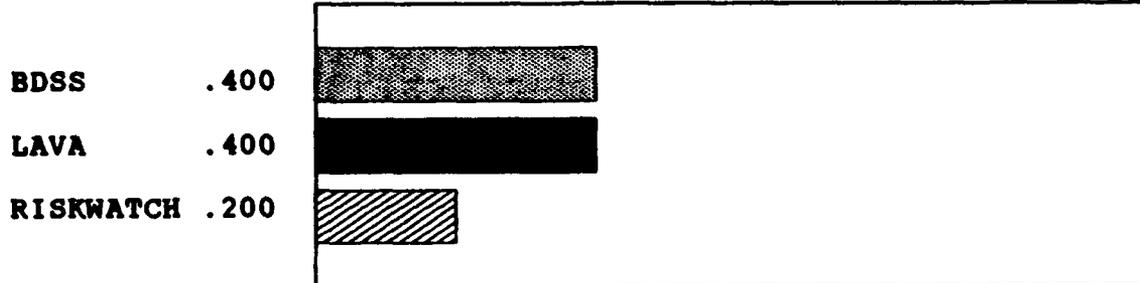


TEMPLATE 14. (continued)

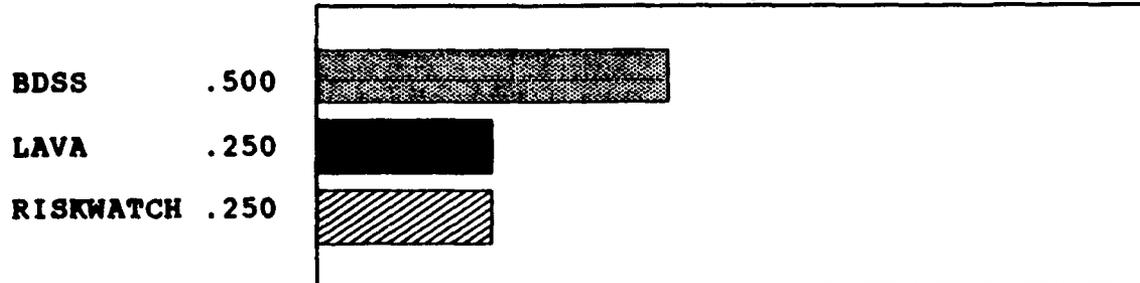
Subsubcriteria: **Comprehensively Considering Safeguards**



Subsubcriteria: **Comprehensively Considering Vulnerabilities**

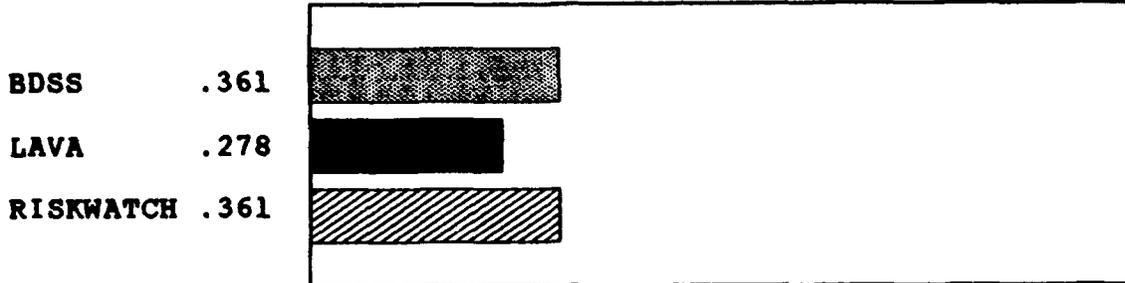


Subsubcriteria: **Considering Outcomes**

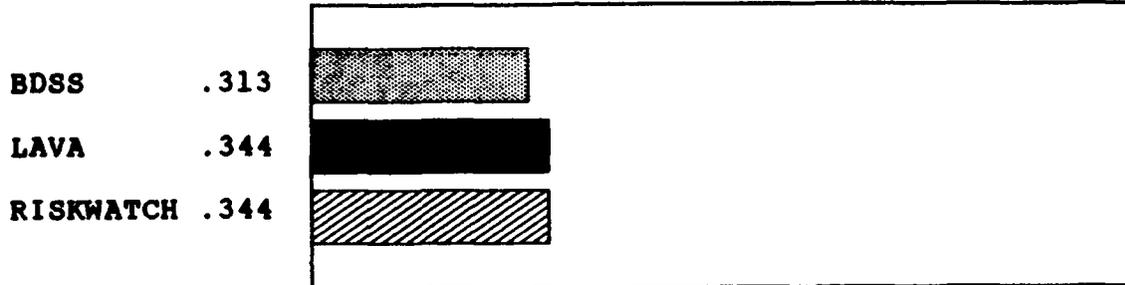


TEMPLATE 15.

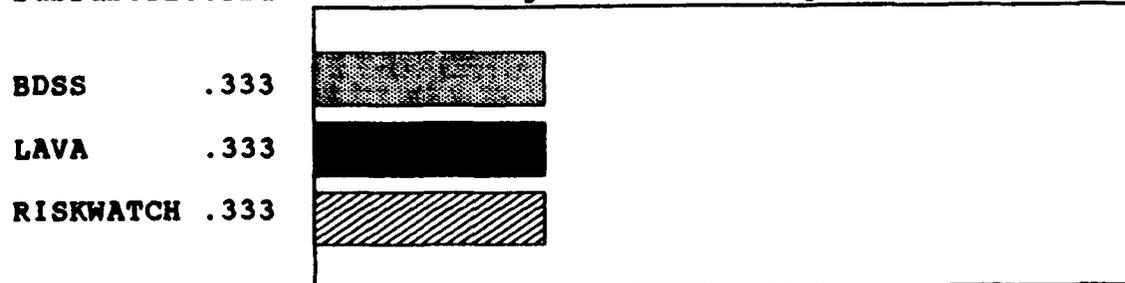
Criteria: Completeness
Subcriteria: Attributes
Subsubcriteria: Considering Asset Values



Subsubcriteria: Considering Potency of Threat Agents

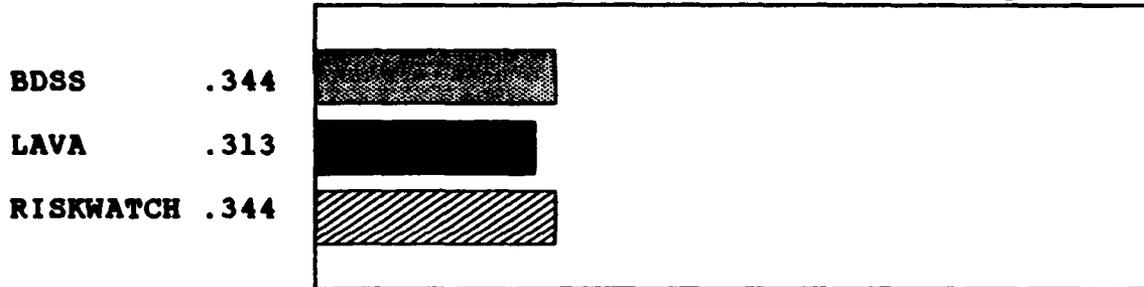


Subsubcriteria: Considering Undesirability of Threat Events

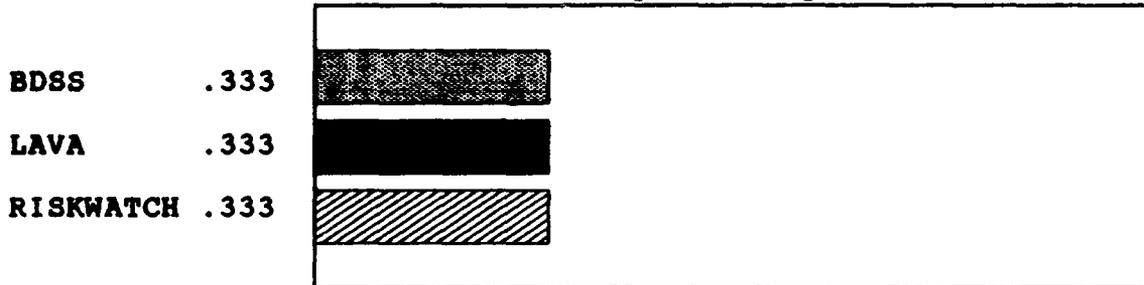


TEMPLATE 15. (continued)

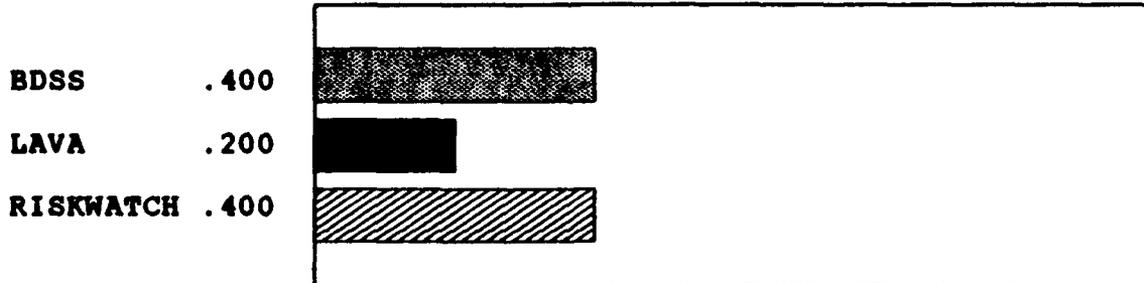
Subsubcriteria: Considering Effectiveness of Safeguards



Subsubcriteria: Considering Severity of Outcomes



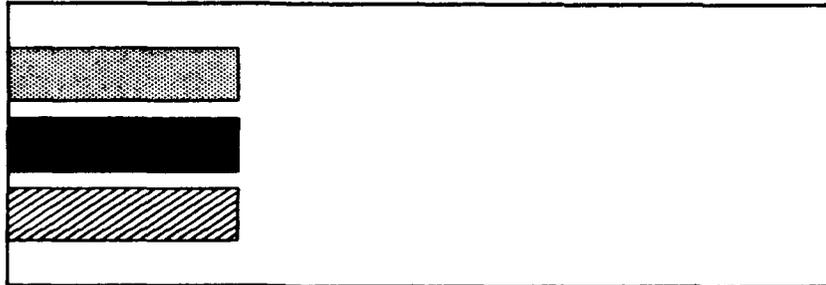
Subsubcriteria: Considering Probabilities of the Occurrence of Threat Events



TEMPLATE 16.

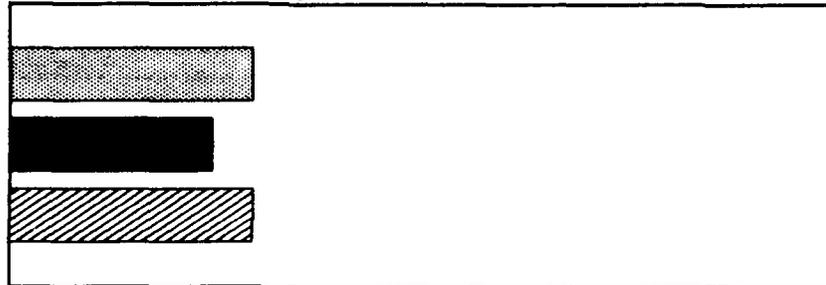
Criteria: Validity
Subcriteria: Relevancy
Subsubcriteria: Expressing Results in Terms of Solutions
Rather than Specifics

BDSS .333
LAVA .333
RISKWATCH .333



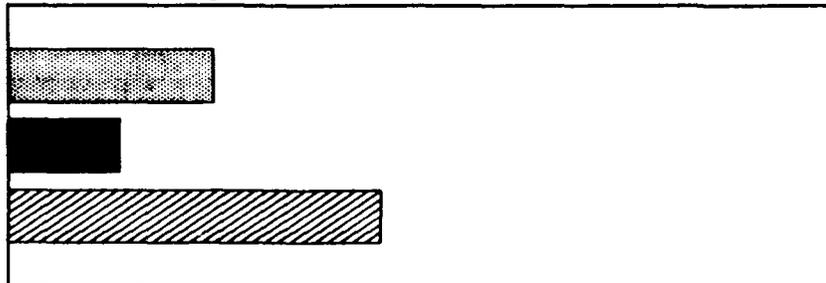
Subsubcriteria: Results Relating to Significant Areas of Need

BDSS .353
LAVA .294
RISKWATCH .353



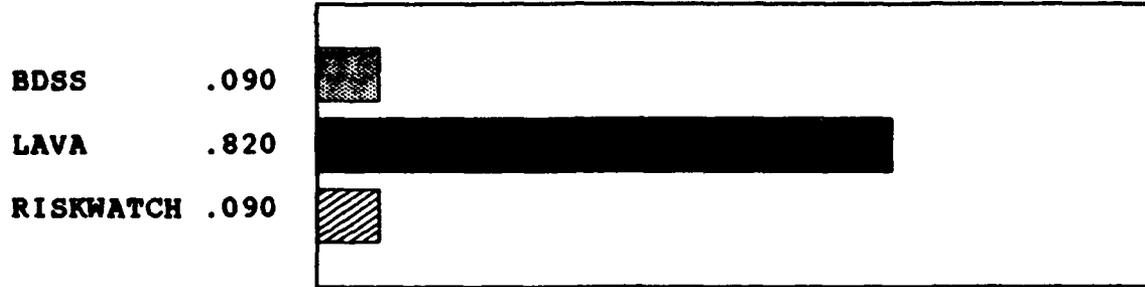
Subsubcriteria: Results Fulfilling Mandated Requirements and Regulations

BDSS .297
LAVA .163
RISKWATCH .540

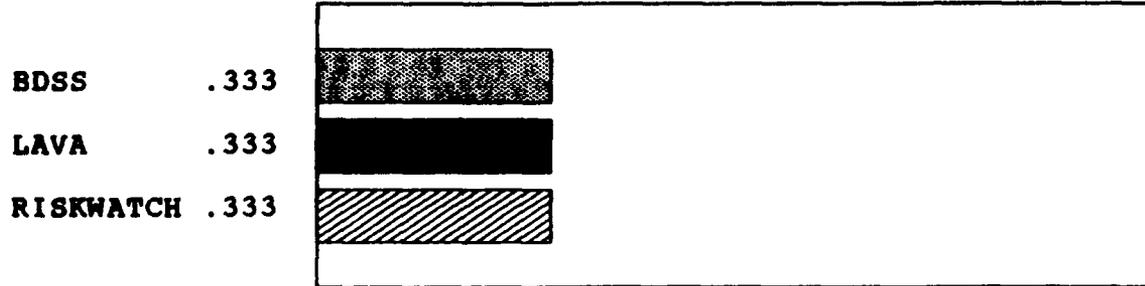


TEMPLATE 16. (continued)

Subsubcriteria: Output Results Being Qualitative

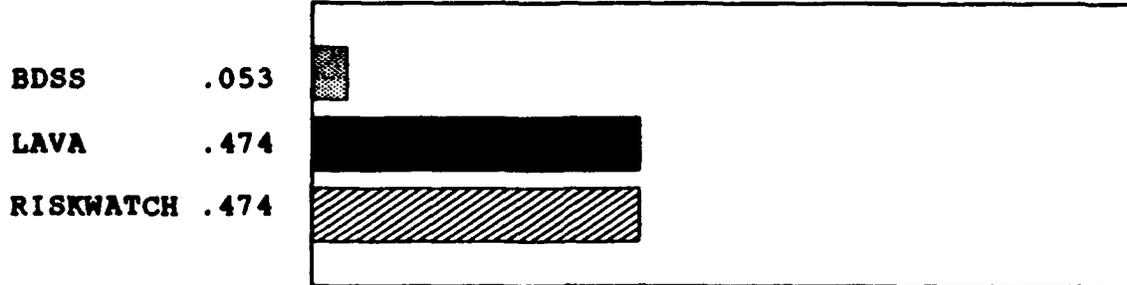


Subsubcriteria: Output Results Being Quantitative

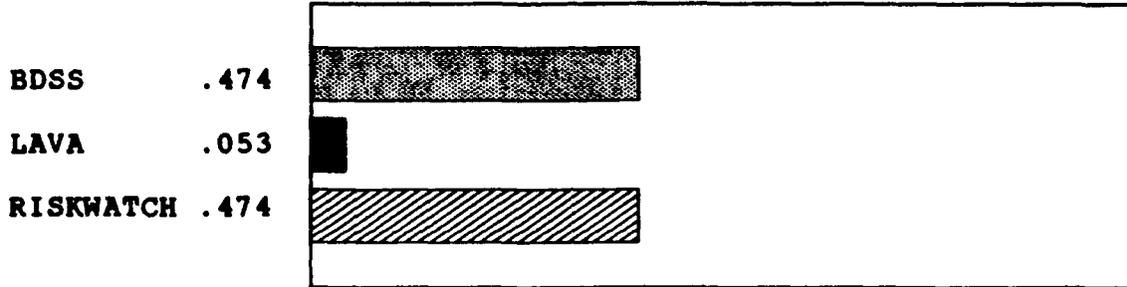


TEMPLATE 17.

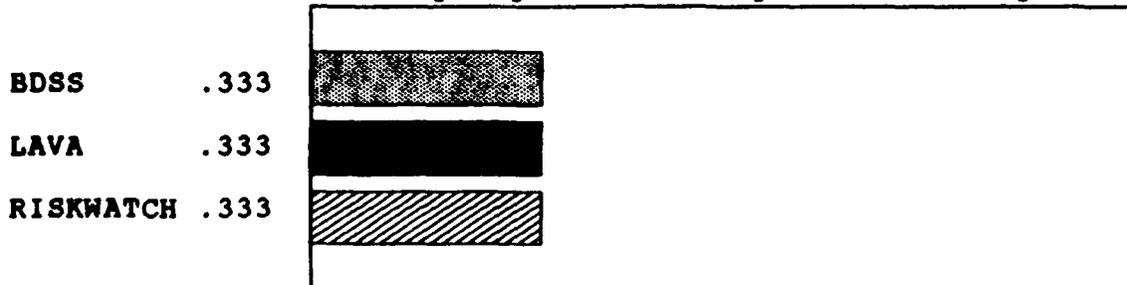
Criteria: Validity
Subcriteria: Scope
Subsubcriteria: User Selecting Amount of Detail



Subsubcriteria: Bounding Detail at the Level Desired

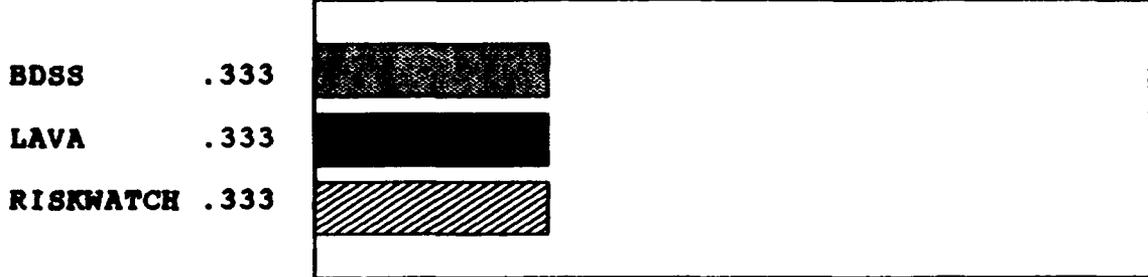


Subsubcriteria: Analyzing All Data Aspects of the System

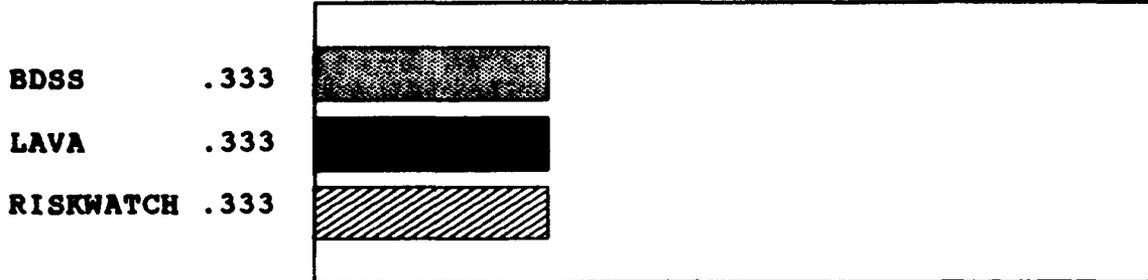


TEMPLATE 17. (continued)

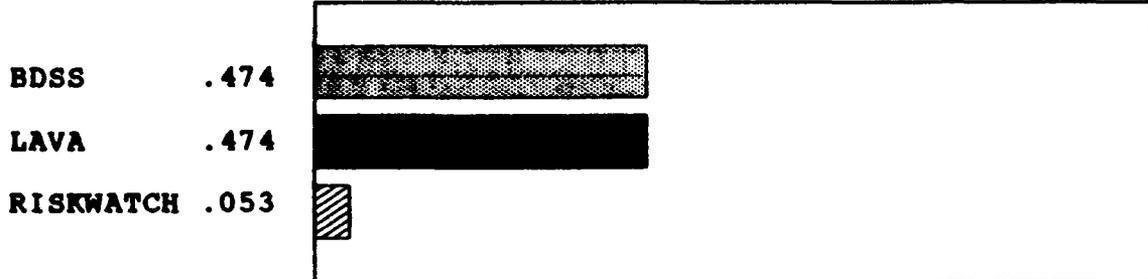
Subsubcriteria: Analyzing Procedural Aspects of the System



Subsubcriteria: Analyzing Personnel Aspects of the System



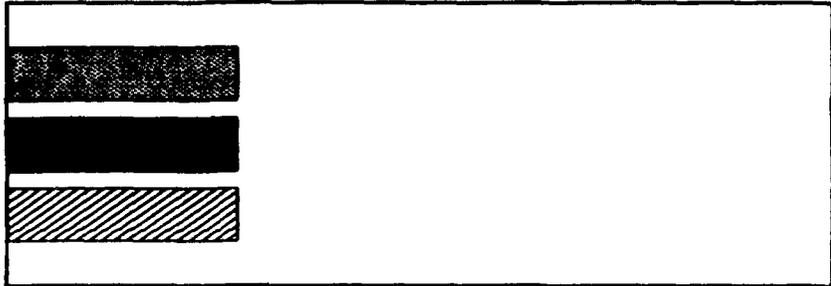
Subsubcriteria: Analyzing Communication Aspects of the System



TEMPLATE 17. (continued)

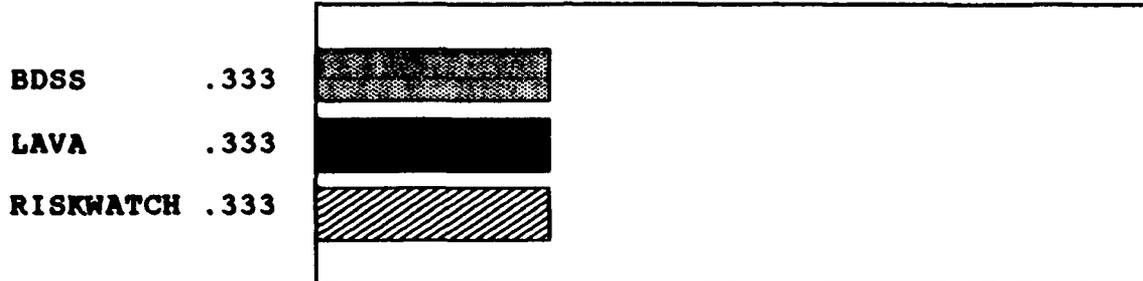
Subsubcriteria: Analyzing Environment of the System

BDSS .333
LAVA .333
RISKWATCH .333

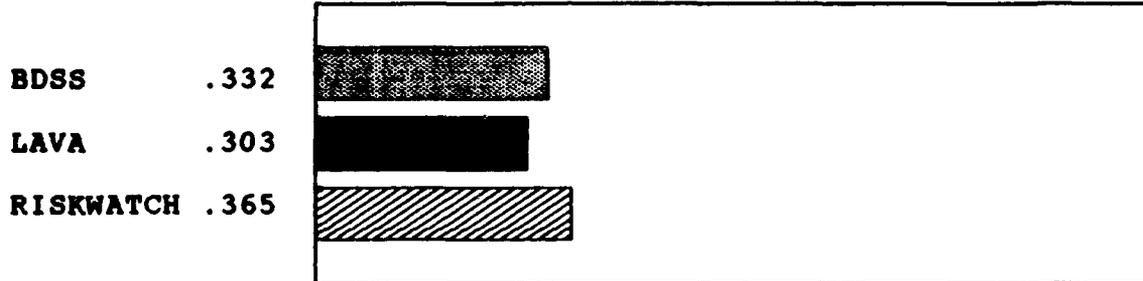


TEMPLATE 18.

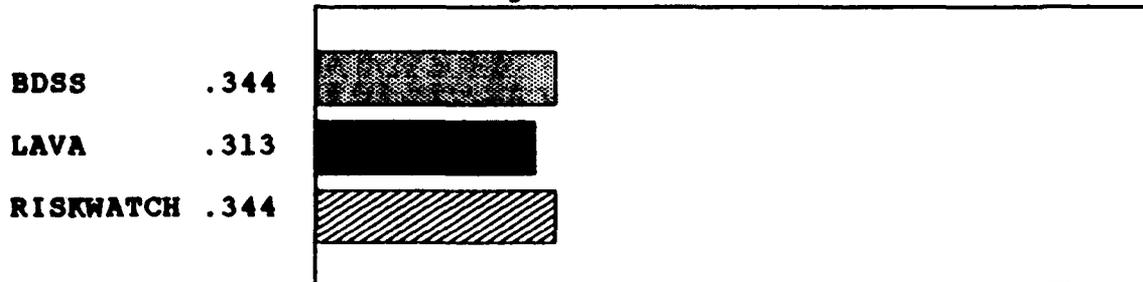
Criteria: Validity
Subcriteria: Practicality
Subsubcriteria: Allowing Input in a Variety of Forms



Subsubcriteria: Performing the Process by Available Staff



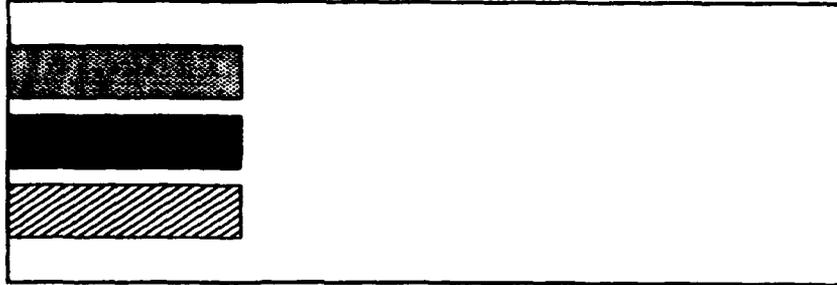
Subsubcriteria: Time Being Available to Perform the Process



TEMPLATE 18. (continued)

Subsubcriteria: Obtaining Precision Economically

BDSS .333
LAVA .333
RISKWATCH .333



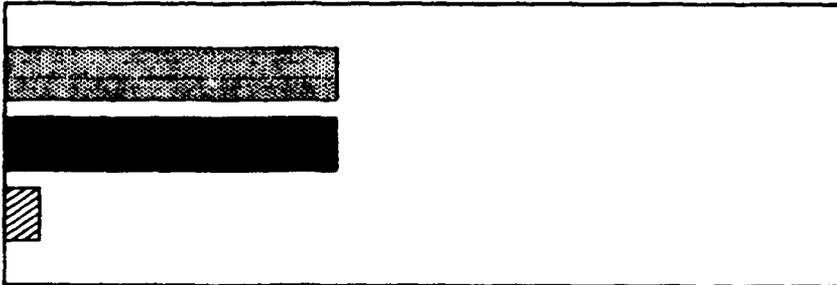
Subsubcriteria: Analyzing Personnel Aspects

BDSS .333
LAVA .333
RISKWATCH .333



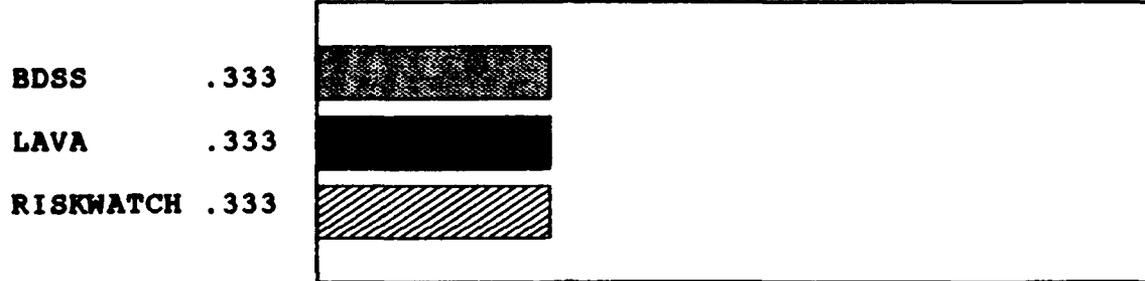
Subsubcriteria: Analyzing Communication Aspects

BDSS .474
LAVA .474
RISKWATCH .053



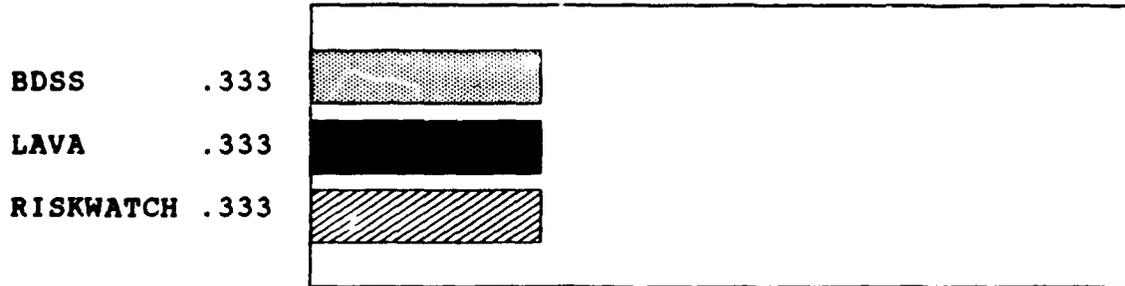
TEMPLATE 18. (continued)

Subsubcriteria: Analyzing Environment Aspects

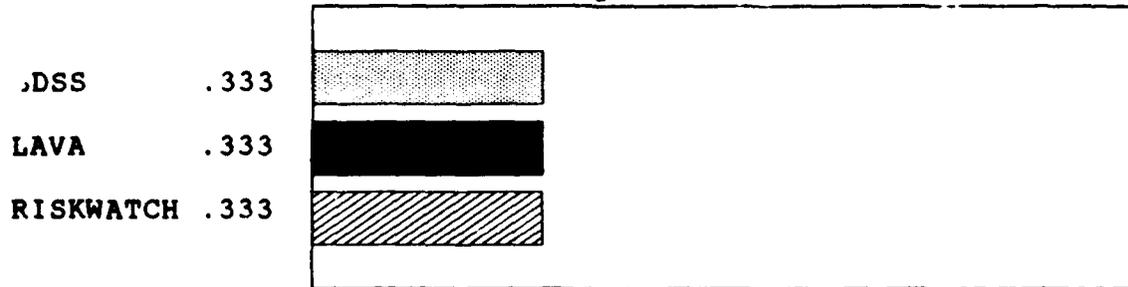


TEMPLATE 19.

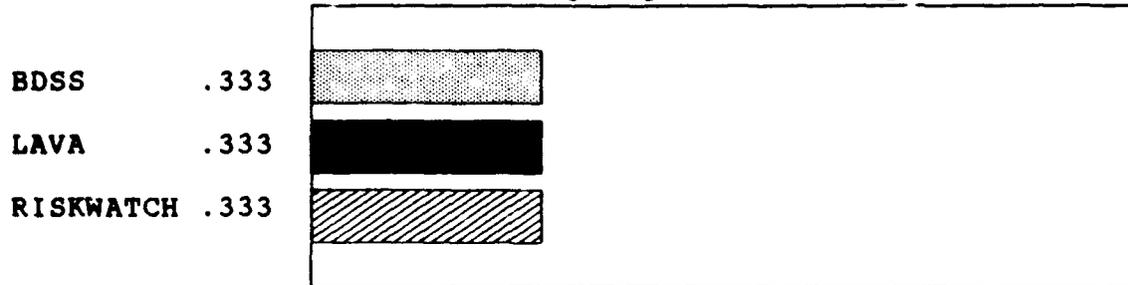
Criteria: Credibility
Subcriteria: Intuitiveness
Subsubcriteria: Delineating the Relationships Between the Results



Subsubcriteria: Output Being a Perceivable Relationship With the Inputs

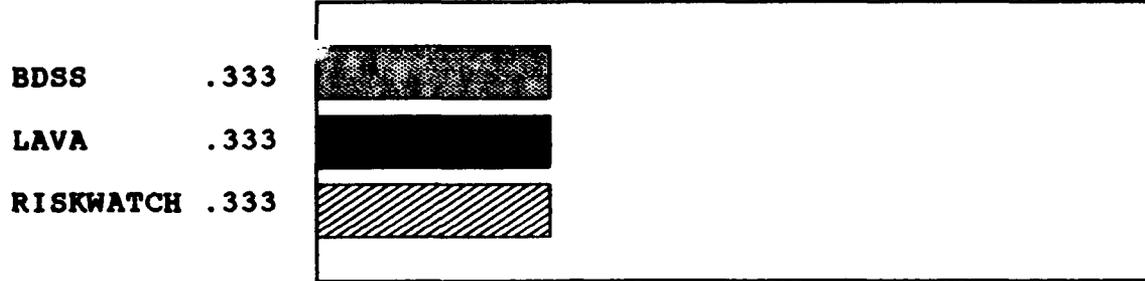


Subsubcriteria: Analyzing All Data Aspects



TEMPLATE 19. (continued)

Subsubcriteria: Analyzing Procedural Aspects



TEMPLATE 20.

Criteria: Credibility
Subcriteria: Reliability
Subsubcriteria: Reducing the Introduction of Personal Bias

BDSS .333

LAVA .333

RISKWATCH .333

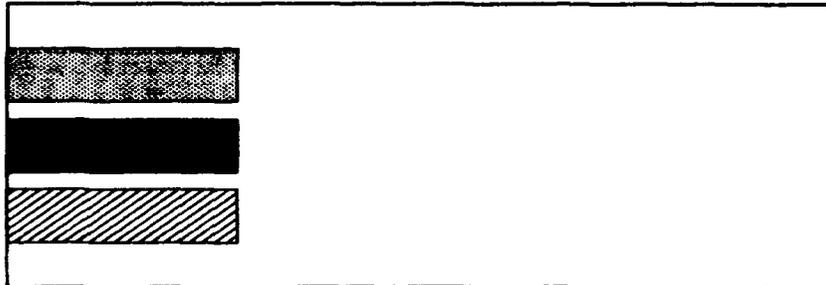


Subsubcriteria: Reducing the Impact of Uncertainty

BDSS .333

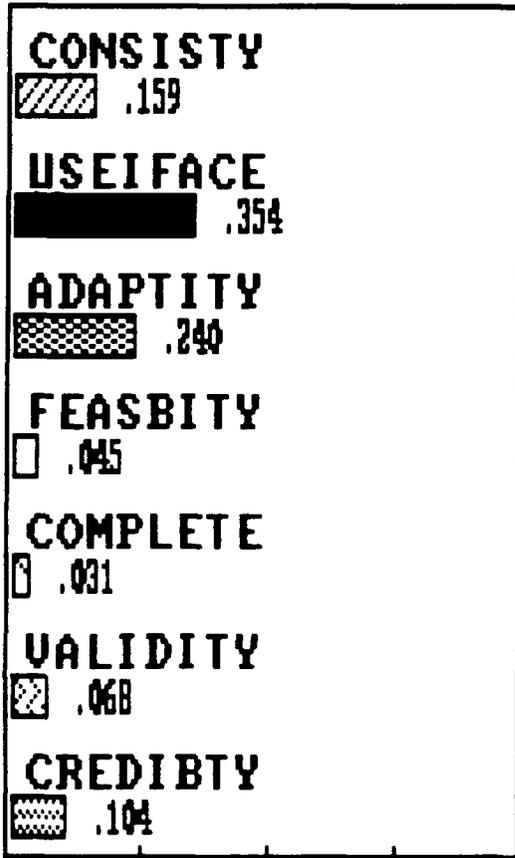
LAVA .333

RISKWATCH .333

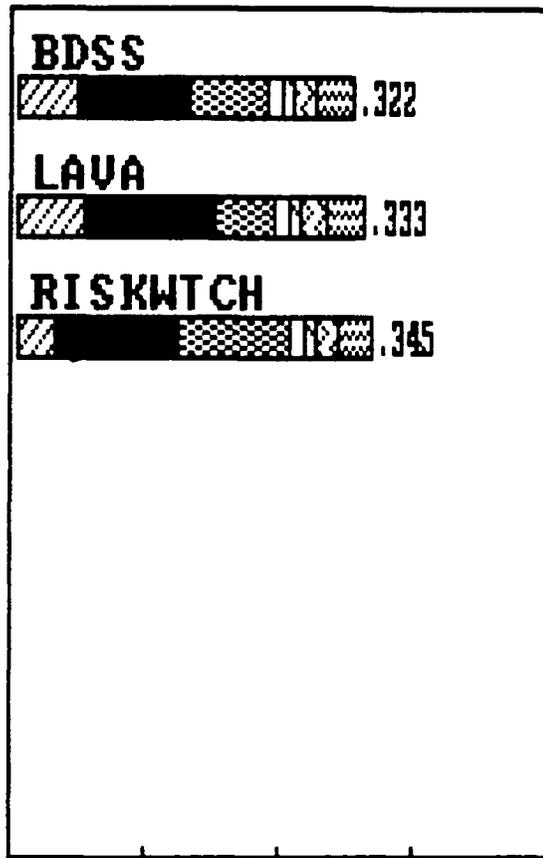


TEMPLATE 2.

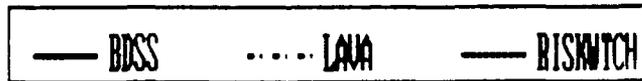
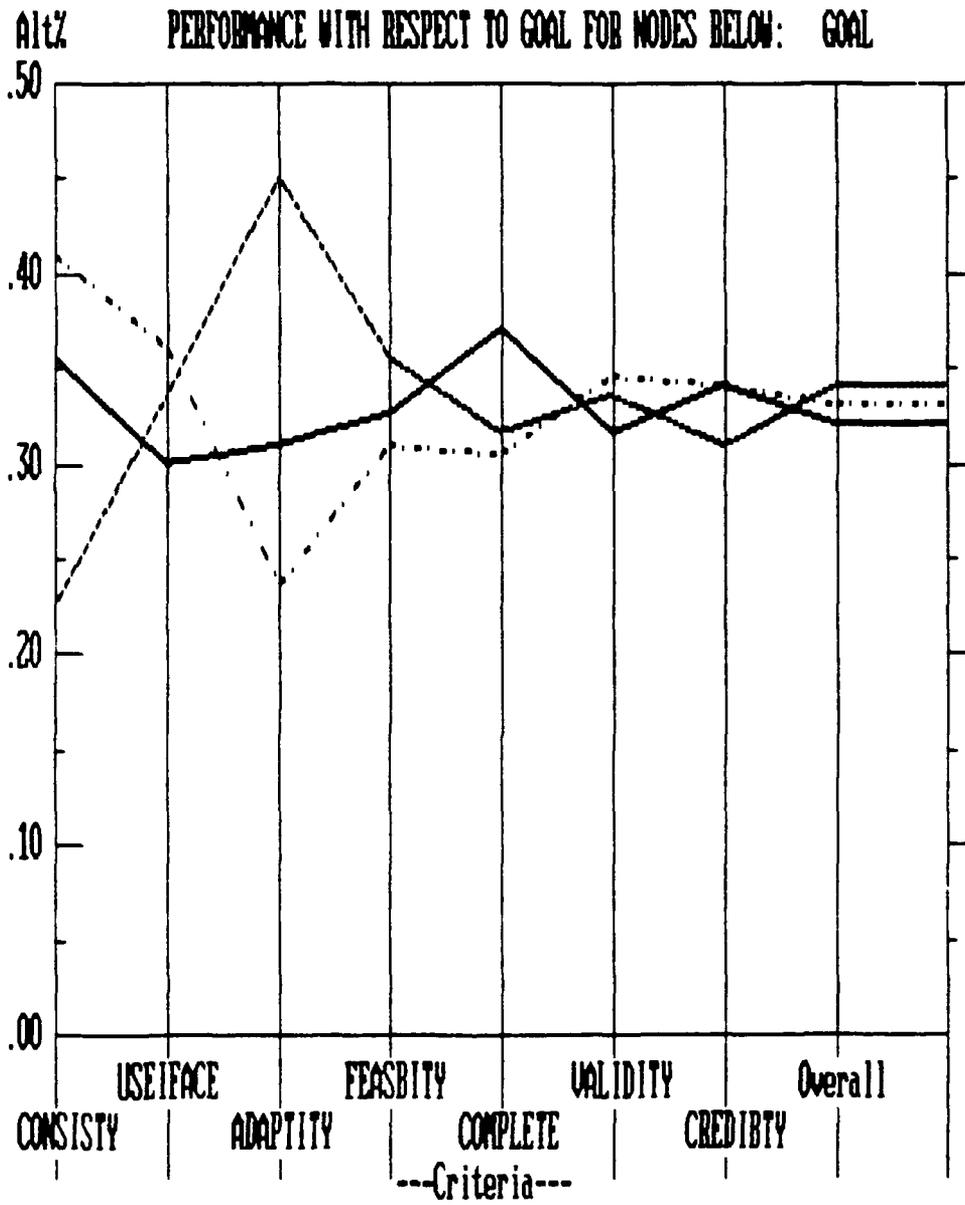
CRITERIA



ALTERNATIVES



TEMPLATE 3.



TEMPLATE 4.

CRITERIA

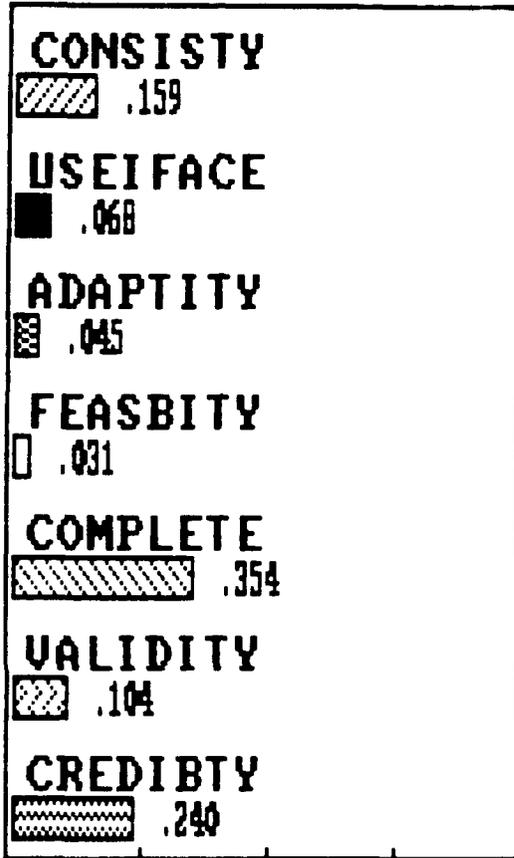
CONSISTY	 .219
USEIFACE	 .329
ADAPTITY	 .223
FEASBITY	 .042
COMPLETE	 .029
VALIDITY	 .063
CREDIBTY	 .096

ALTERNATIVES

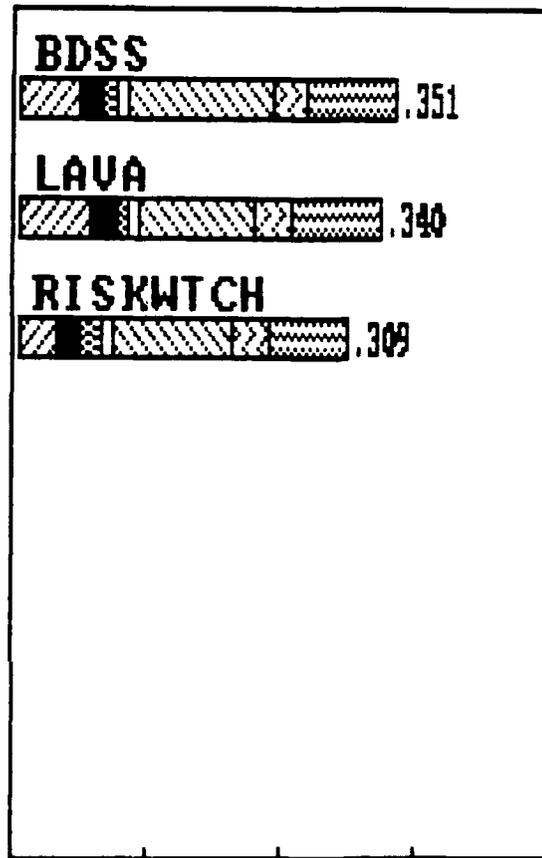
BDSS	    .325
LAVA	    .339
RISKWTCH	    .336

TEMPLATE 2.

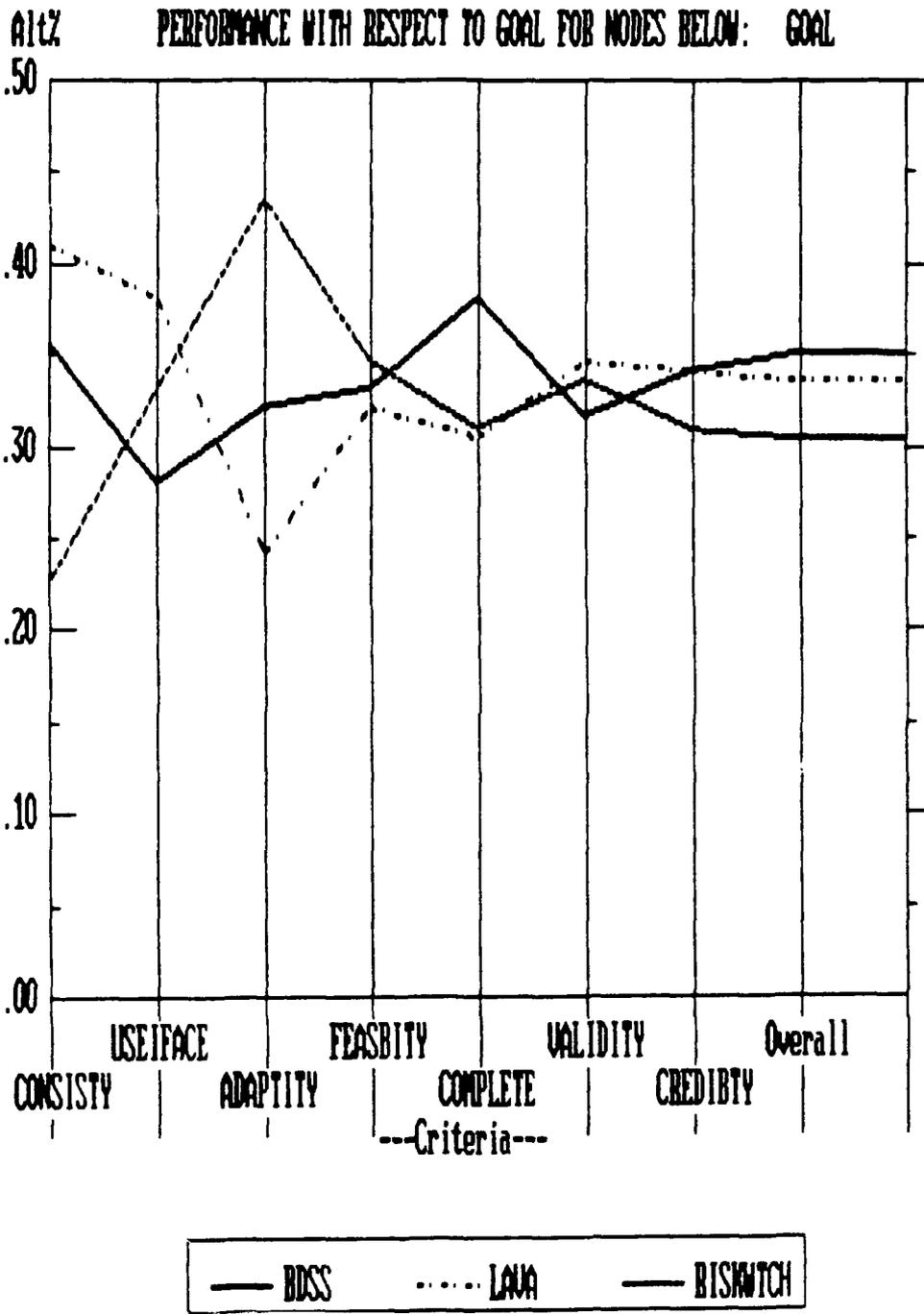
CRITERIA



ALTERNATIVES

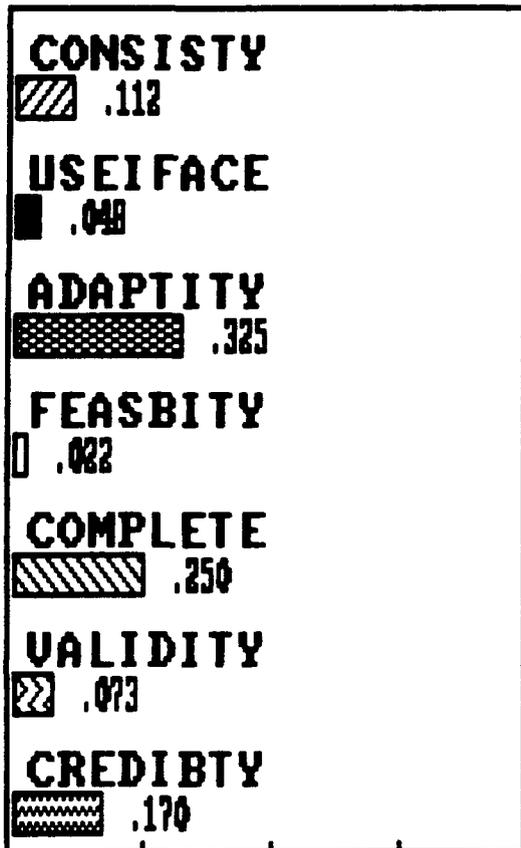


TEMPLATE 3.

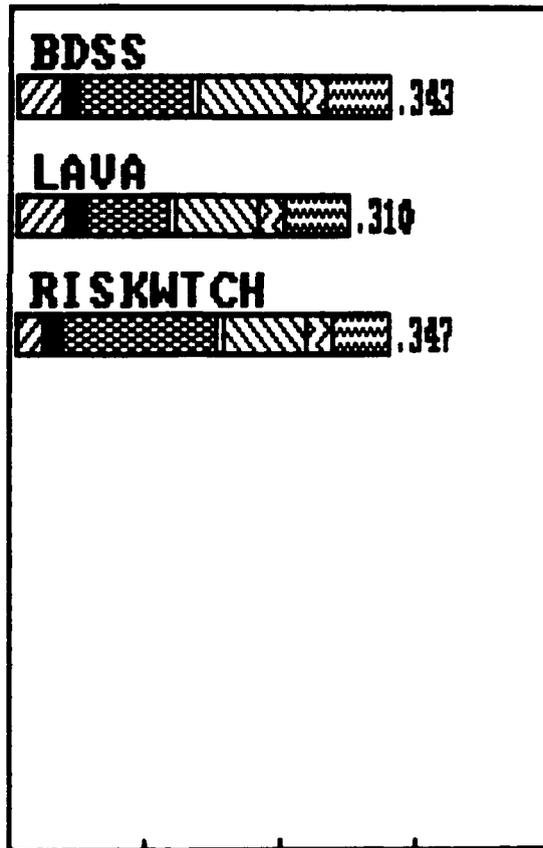


TEMPLATE 4.

CRITERIA

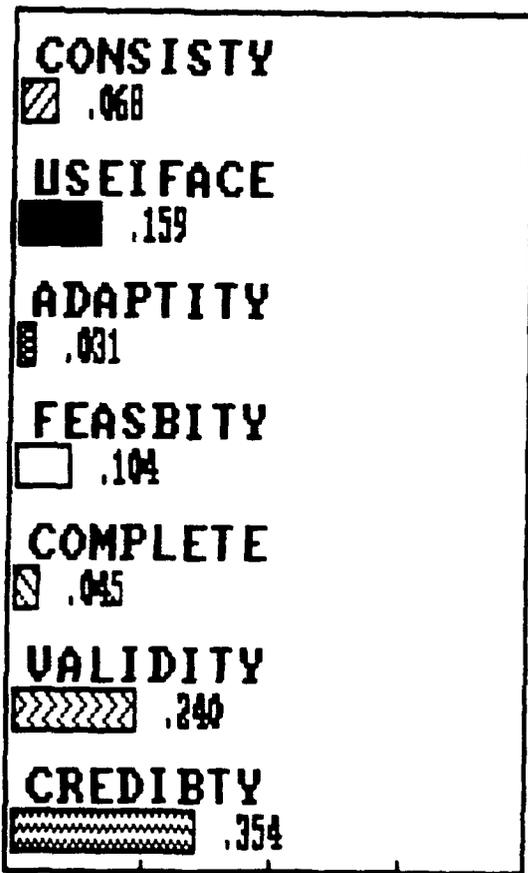


ALTERNATIVES

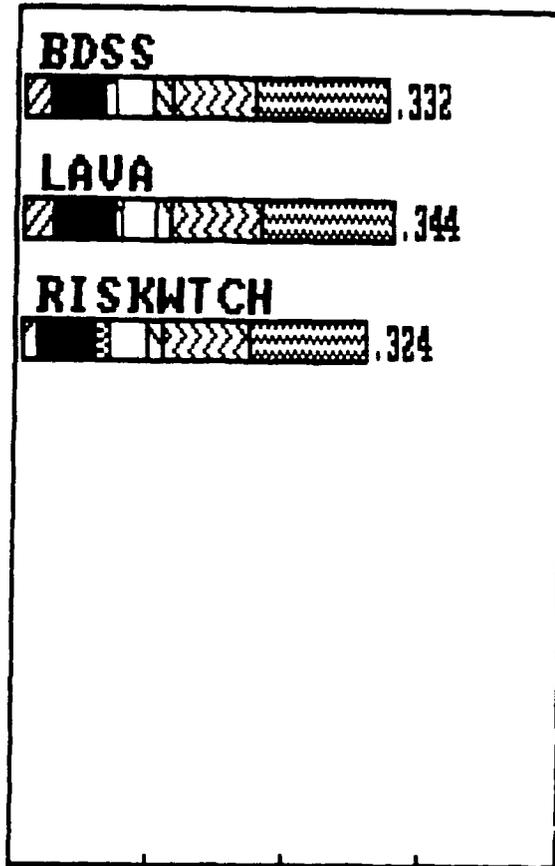


TEMPLATE 2.

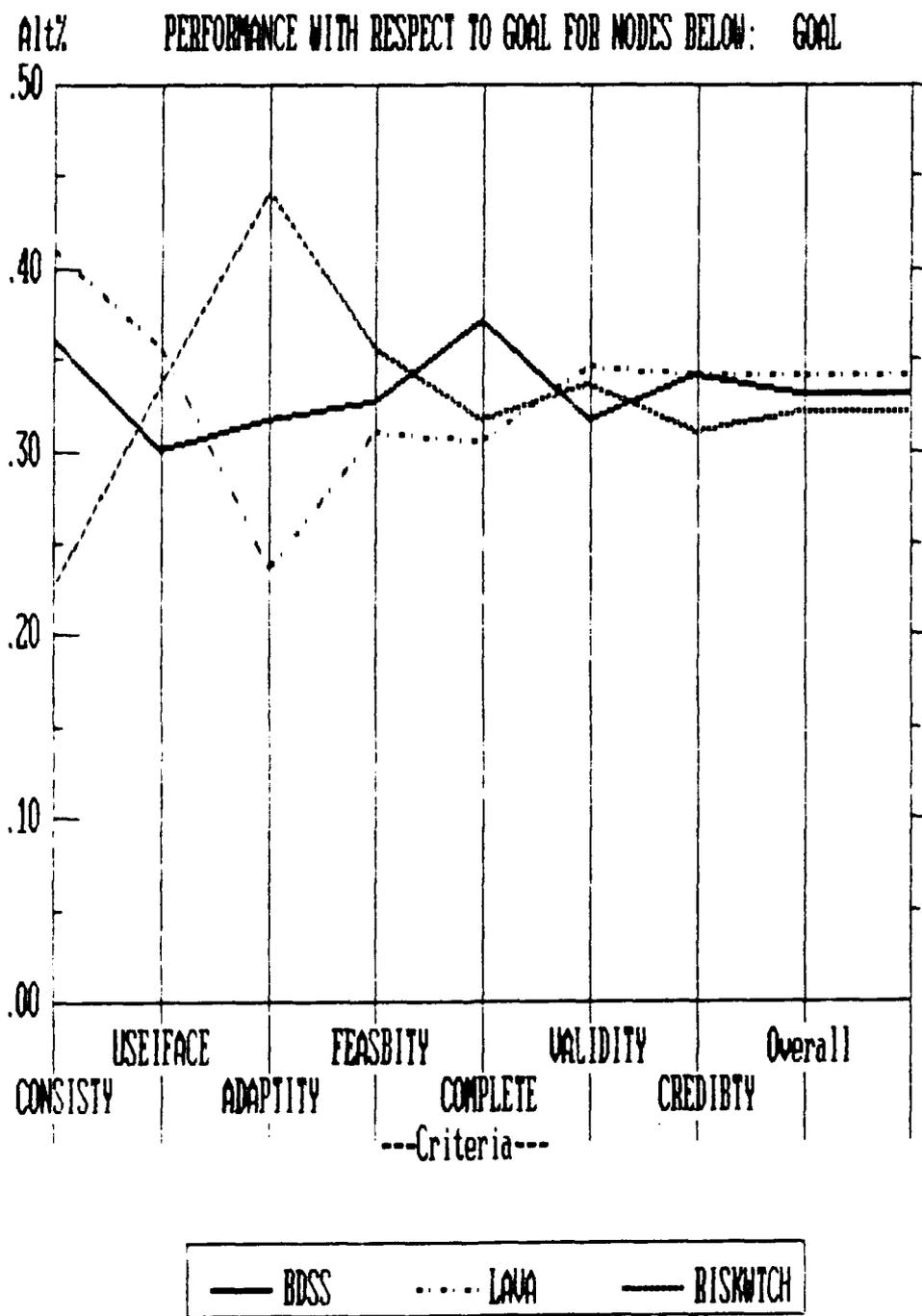
CRITERIA



ALTERNATIVES

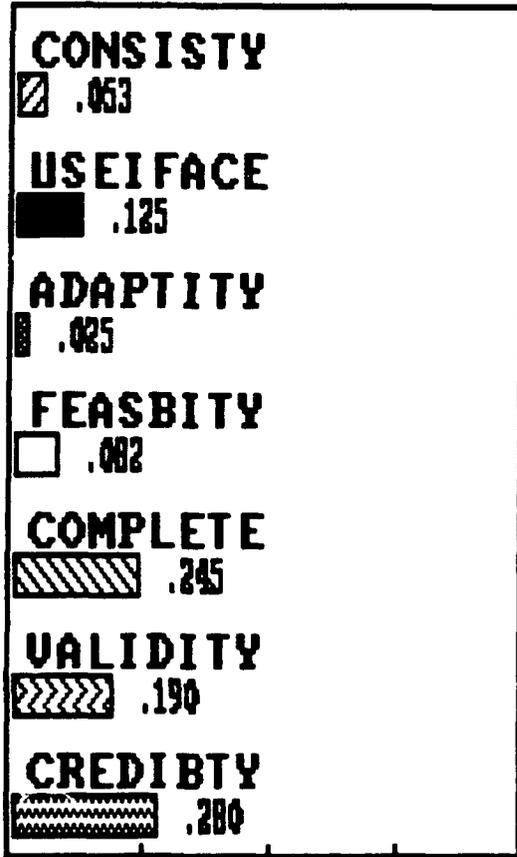


TEMPLATE 3.

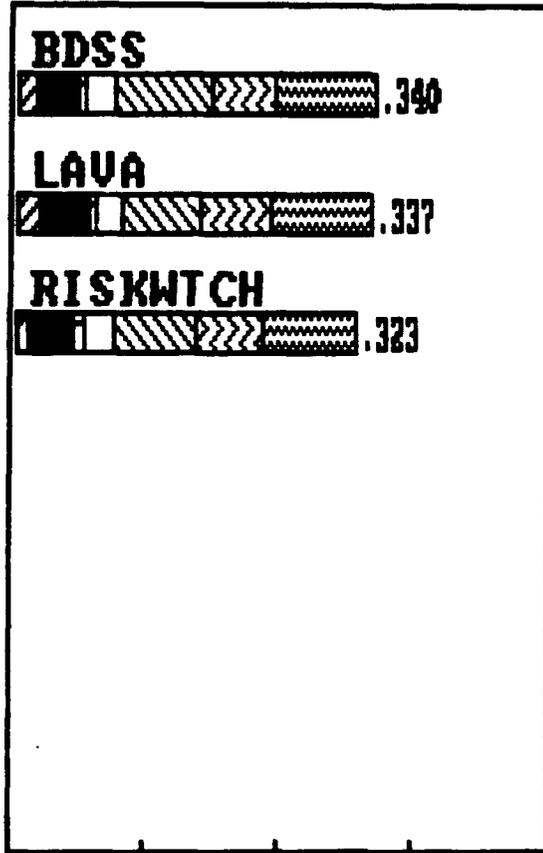


TEMPLATE 4.

CRITERIA



ALTERNATIVES



LIST OF REFERENCES

- Buck, Edward R. Introduction to Data Security and Controls. Q.E.D. Information Services, Inc., 1982.
- Clements, Donald Paul. Fuzzy Ratings for Computer Security Evaluation. UMI Dissertation Information Service, 1977.
- Computer Security. U.S. Department of Commerce National Technical Information Service PB-290 896.
- Computer Security. U.S. Office of Management and Budget. February, 1979.
- Cooper, Dale, and Chris Chapman. Risk Analysis for Large Projects. John Wiley & Sons, 1987.
- Covello, Vincent T., Joshua Menkes, and Jeryl Mumpower. Risk Evaluation and Management. Plenum, 1986.
- Covello, Vincent T., Lester B. Lave, Alan Moghissi, and V.R.R. Uppuluri. Uncertainty in Risk Assessment, Risk Management, and Decision Making. Plenum, 1984.
- Crouch, Edmund A.D., and Richard Wilson. Risk/Benefit Analysis. Ballinger, 1982.
- Data on Security of Automated Information Systems That Process Information Related To The National Security Interest. Executive Office of the President, Office of Management and Budget, March 28, 1985.
- Fifth Annual Computer Security Applications Conference. IEEE Computer Society Press, 1990.
- Fischhoff, Baruch, Sarah Lichtenstein, Paul Slovic, Stephen L. Darby, and Ralph L. Keeney. Acceptable Risk. Cambridge University, 1981.
- Frankel, Ernst G. Systems Reliability and Risk Analysis. Kluwer Academic, 1988.
- Garrabrants, W.M., and A.W. Ellis. "CERTS: A Comparative Evaluation Method for Risk Management Methodologies and Tools." 1990.

- Garrabrants, W.M., A.W. Ellis, L.J. Hoffman, and M.N. Kamel, "CERTS: A Comparative Evaluation Method for Risk Management Methodologies and Tools," in Proceedings of the Sixth Annual Computer Security Applications Conference, Tucson, AZ, December, 1990.
- Hoffman, Lance J. Computers and Privacy in the Next Decade. Academic, 1980.
- Hoffman, Lance J. Modern Methods for Computer Security and Privacy. Prentice-Hall, Inc., 1977.
- Hoffman, Lance J. Risk Analysis and Computer Security: Bridging Cultural Gaps. National Computer Security Conference Proceedings, September 15-18, 1986.
- Katzke, S. W. "A Government Perspective on Risk Management of Automated Information Systems," in Proceedings of the 1988 Computer Security Risk Management Model Builder's Workshop, Denver, CO, National Computer Security Center, May, 1988.
- Lave, Lester B. Risk Assessment and Management. Plenum, 1987.
- Mayerfeld, H.T. "Framework for Risk Management: A Synthesis of the Working Group Repots From the First Computer Security Risk Management Model Builder's Workshop," in Proceedings of the 1989 Computer Security Risk Management Model Builder's Workshop, Ottawa, Canada, National Computer Security Center, June, 1989.
- Merkhofer, Miley W. Decision Science and Social Risk Management. D. Reidel, 1987.
- Otwell, Ken, and Bruce Aldridge. The Role of Vulnerability in Risk Management. Fifth Annual Computer Security Application Conference. IEEE Computer Society Press, 1989.
- Palmer, I.C., and G.A. Potter. Computer Security Risk Management. Van Nostrand Reinhold, 1989.
- Patton, Michael Quinn. Qualitative Evaluation Methods. Sage, 1980.
- Pfleeger, Charles P. Security in Comuting. Prentice Hall, 1989.

- Quade, E.S. Analysis for Public Decisions. North Holland, 1982.
- Rullo, Thomas A. Advances in Computer Security Management. Volume 1. Heyden & Sons, Inc., 1980.
- Saaty, T. L., The Analytic Hierarchy Process. McGraw Hill, 1980.
- Saaty, T. L., Decision Making for Leaders. Lifetime Learning, 1982.
- Schmucker, Kurt J. Fuzzy Sets, Natural Language Computations, and Risk Analysis, Computer Science, 1984.
- Tannis, Daryl C. An Assessment of the National Computer Security Center's Approach for Computer Network Security and a Recommended Altrnative Systems Approach. UMI Dissertation Information Service, 1988.
- Walker, Bruce J. and Ian F. Blake. Computer Security and Protection Structures. Dowden, Hutchinson & Ross, Inc., 1977.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
Cameron Station
Alexandria, Virginia 22304-6145
2. Library, Code 52 2
Naval Postgraduate School
Monterey, California 93943-5002
3. Computer Technology Curricular Office 1
Code 37
Naval Postgraduate School
Monterey, California 93943
4. Magdi Kamel 2
Department of Administrative Science, Code AS/KA
Naval Postgraduate School
Monterey, California 93943
5. Lance J. Hoffman 1
Department of Electrical Engineering
and Computer Science
George Washington University
Washington, D.C. 20052
6. Major Leonard A. Crump Jr. 2
8507 Shirley Woods Court
Lorton, Virginia 22079
7. Lieutenant James G. Pound 2
P.O. Box 126
Fairbanks, Indiana 47849
8. Defense Technical Information Center 1
Attention: Selection Section (DTIC-FDAC)
Building 5, Cameron Station
Alexandria, Virginia 22304-6145
9. Irene Gilbert 1
National Institute of Standards and Technology
Gaithersburg, Maryland 20899
10. Nicki Lynch 1
National Institute of Standards and Technology
Gaithersburg, Maryland 20899