PB84-171321

# Guidelines for Developing NASA (National Aeronautics and Space Administration) ADP Security Risk Management Plans

MITRE Corp., McLean, VA. METREK Div

Prepared for

National Aeronautics and Space Administration
Washington, DC

Aug 83

# Guidelines for Developing NASA ADP Security Risk Management Plans

Frederick G. Tompkins

August 1983

MTR-83W123

SPONSOR:
NASA
CONTRACT NO.:
NASW-3425
PROJECT NO.:
1915F
DEPT.:
W-27

The MITRE Corporation
Metrek Division
1820 Dolley Madison Boulevard
McLean, Virginia 22102

50272-101

**REPORT DOCUMENTATION PAGE**

1. REPORT NO.

2.

3. Recipient's Accession No.
PB84 171321

4. Title and Subtitle
GUIDELINES FOR DEVELOPING NASA AND SECURITY RISK MANAGEMENT PLANS

5. Report Date
AUGUST 1983

6.

7. Author(s)
Frederick G. Tompkins

8. Performing Organization Rept. No.
MTR-83W123

9. Performing Organization Name and Address
The MITRE CORPORATION
Metrek Division
1820 Dolley Madison Boulevard
McLean, VA 22102

10. Project/Task/Work Unit No.
1915F

11. Contract(C) or Grant(G) No.
(C) NASW-3425
(G)

12. Sponsoring Organization Name and Address
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
400 Maryland Avenue, SW
Washington, DC 20546

13. Type of Report & Period Covered
FINAL

14.

15. Supplementary Notes

16. Abstract (Limit: 200 words)

This report presents guidance to NASA Computer security officials for developing ADP security risk management plans. The six components of the risk management process are identified and discussed. Guidance is presented on how to manage security risks that have been identified during a risk analysis performed at a data processing facility or during the security evaluation of an application system.

17. Document Analysis a. Descriptors
Computer security, ADP security, risk analysis, risk assessment, risk management

b. Identifiers/Open-Ended Terms

c. COSATI Field/Group

18. Availability Statement:
Kelease Unlimited

19. Security Class (This Report)
UNCLASSIFIED

20. Security Class (This Page)

21. No. of Pages
58

22. Price

(See ANSI-Z39.18)

See Instructions on Reverse

MITRE Department
and Project Approval: R. L. [illegible]

for W. T. Bisignani

This document has been peer reviewed by:

Marshall D Abrams

Marshall D. Abrams

Charles E. Fritz

Charles E. Fritz

## ABSTRACT

The NASA Computer Security Program is based on the fundamental premise that it is not possible to have a risk-free data processing operation. Risks, therefore, must be managed. This report presents guidance to NASA computer security officials for developing risk management plans. An overview of ADP security risk management provides a discussion of the six components of the risk management process: (1) risk analysis, (2) risk reduction analysis, (3) management decisions, (4) risk reduction action plans, (5) implementation and maintenance of plans, and (6) review and audit of plans.

## ACKNOWLEDGEMENT

The author wishes to thank R. S. Rice of NASA who provided assistance to MITRE during the writing of this report and the following individuals who provided background information: Bob Martian of General Electric Corporation; Howerd Keough, McAuto Systems; T. Atwell, Boeing Computer Services and G. Mevius, Peer Services, Inc. The author would also like to thank MITRE associates M. D. Abrams, W. T. Bisignani, C. Fritz and J. Sprung for review and suggestions for the final report and M. Bashioum and C. Neperud for editorial suggestions and clerical support.

## TABLE OF CONTENTS

## TABLE OF CONTENTS

(con⁻luded)

## LIST OF ILLUSTRATIONS

# 1. INTRODUCTION

The Office of Management and Budget (OMB) Circular A-71, Transmittal Memorandum No. 1, dated 27 July 1978, requires each agency to develop and implement a computer security program. This document provides guidance for developing risk management plans which are one aspect of the NASA Computer Security Program. The development, implementation, and maintenance of risk management plans follow the performance of a Data Processing Installation (DPI) risk analysis or a sensitive application evaluation and certification process. Risk management planning is performed to assure that ADP security risks are prudently managed since it is not possible to have a risk-free data processing environment.

NASA is well into the computer security program development and implementation process in compliance with OMB Circular A-71, TM No. 1. NASA Management Instruction (NMI) 2410.7, "Assuring Security and Integrity of NASA Data Processing" has been issued; Center-level management instructions on computer security have been issued; Computer Security Officials (CSOs) at the Center, DPI and applications levels have been appointed; and computer security guidelines have been published to address the performance of risk analysis, definition of security requirements for applications software, evaluation/certification of existing applications software, ADP contingency planning and computer security training. Also, a number of DPI risk analyses and application certifications have been accomplished.

One of the next steps in the implementation of the NASA Computer Security Program is to develop guidance on managing the security risks associated with their data processing installations and applications systems. The guidance provided herein may be modified by the NASA Centers, individual NASA DPIs, or, with NASA approval, by the NASA contractors who develop risk management plans for NASA organizations. The guidance and risk management process may also be modifed to suit the needs of a DPI or an application commensurate with the nature and degree of identified risk.

## 1.1 Purpose

The purpose of this document is to provide NASA Center, DPI, and Sensitive Application CSOs with guidance on the preparation, implementation and maintenance of risk management plans (RMPs). These plans must be adequate to meet federal and agency requirements and provide a systematic and flexible approach to managing computer security risks. This document addresses the risk management planning which should be accomplished at the data processing installation, application software, and Center levels.

## 1.2 Scope

The guidelines presented in this document provide a systematic process to assure that the security risks reported to NASA management are acted upon in an orderly and timely fashion. Implementation of controls should be accomplished according to a cohesive plan approved by top management. The guidance is applicable to the management of security risks that have been identified during a risk analysis performed at a data processing installation or during the evaluation/certification of a sensitive application.

## 1.3 Key Action Items in Risk Management Planning

Computer security officials, in their role as risk managers or risk management planners, must accomplish a series of actions to assure that DPI and application risk management plans are both comprehensive and usable. Lack of proper planning may result in the implementation of ineffective controls, improper implementation of controls, or a plan that is not responsive to changes in mission, organization, technology, and personnel. The action items that should be accomplished by risk management plan developers, implementers, and maintainers are:

1. Define the Risk Environment.* Review and document current equipment and facility configurations; identify sensitive and critical applications; and understand the data processing operating environment.

2. Define the Categories of Risk.* The threats that can adversely impact a DPI or an application should be identified and documented.

3. Evaluate Occurrence of Risks.* Each documented risk should be evaluated with respect to its likelihood of occurrence. The rationale for the likelihood should also be documented for future reference.

4. Assessment of Risk Occurrence Impact.* Assess and document the impact on the DPI or application for each risk, should it materialize.

5. Document Risk Reduction Decisions. The decisions made by management following a DPI risk analysis or an application evaluation should be documented. The controls selected for implementation, budgetary limitations, and the milestones set by management should be included in the documentation.

6. Develop Risk Reduction Action Plan. The risk reduction action plan details the specific controls as action

*The first four action items collectively comprise a risk analysis or evaluation/certification activity.

items to be implemented. It also details the schedule for internal design development, installation, and/or procurement. The plan also establishes responsibility for the accomplishment of each action item.

7. Implement the Controls. Implementation will involve integration of new/revised controls into existing processes. Personnel should be briefed or trained in the operation of new controls. The rationale and benefits to be derived from implementation should also be explained.

8. Develop Risk Management Plan Maintenance Procedures. Changes in technology, organizations, and individuals will probably cause changes to be made in the security requirements of the DPI and the applications. Maintenance procedures should be developed to ensure that the risk management plan remains a dynamic and viable management tool.

9. Review and Audit. The risk management plan must be reviewed periodically to determine if action items are being accomplished in accordance with the plan. Changes in facilities, equipment; organization, or personnel may require modification to the risk management plan. Changes may also indicate an update of the last risk analysis and application evaluation should be considered.

## 1.4 Overview of the Report

Section 2 provides an overview of risk management concepts and the risk management planning process. Section 3 presents a discussion of the steps to be accomplished in developing DPI, application and Center risk management plans. Section 4 addresses the area of risk management plan maintenance.

## 2. OVERVIEW OF RISK MANAGEMENT

NASA Handbook (NHB) 2410.1, Computer Resources Management, Appendix J, states:

> ... the NASA Computer Security program is based on the fundamental premise that it is not possible to have a risk-free data processing environment. Risks, therefore, must be managed. They must be appropriately defined, categorized as to likelihood of occurrence, and assessed as to the resultant consequences if they occur. Actions must then be taken to allocate resources to minimize risks in a manner that provides the best overall security.

Risk management is a comprehensive concept for defining and analyzing the threats of which we are aware and assisting management in optimizing the amount of security return on the investment dollar. The risk management process attempts to answer the following questions:

- What is at risk and what needs to be done?
- What security controls are available to reduce the risks?
- What security controls will provide the best return on investment?
- Who is responsible for implementation?
- How will controls be implemented and over what time frame?
- How effective are the controls once they are installed?

The ADP security risk management process consists of six major phases:

1. Risk Analysis
2. Risk Reduction Analysis

3. Management Decision
4. Development of Risk Reduction Action Plans
5. Implementation and Maintenance of Controls
6. Review and Audit

The ADP security risk management process provides for progressive iteration since the risk environment is subject to change. Figure 2-1 depicts the process, the questions which are answered in each phase, and the iterative nature of the process. The ADP security risk management process is based on the fundamental risk management concepts and definitions.

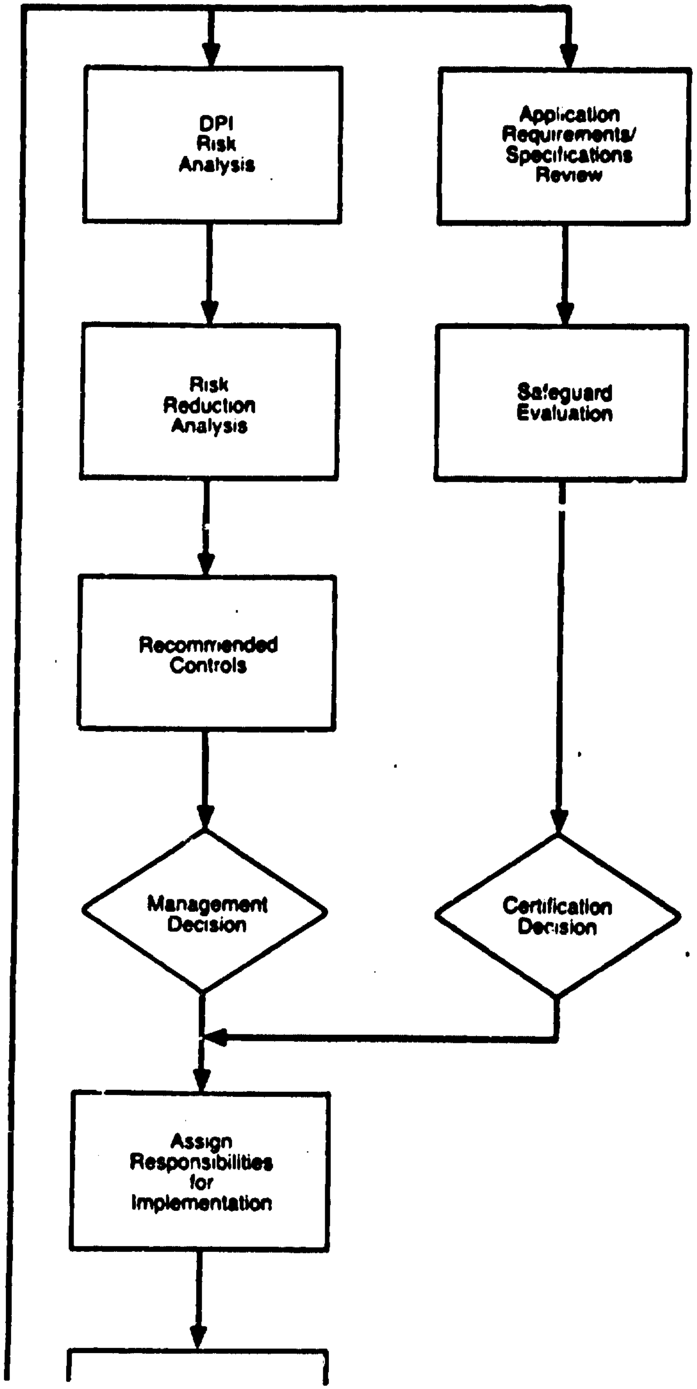
## 2.1 Risk Management Concepts

In "An Anatomy of Risk," William D. Rowe introduces the concept of risk with the following statement:

> The only certainty in life is death; uncertainty lies in when and how death occurs, and whether it is final. Man strives to delay its onset and extend the quality of life in the interim. Threats to these objectives involve risks, some natural, some man-made, some beyond our control, and some controllable.

Rowe further states:

> Everyone is constantly subjected to an array of risks, both as an individual and as a member of various societal groups. Generally these risks are accepted qualitatively, even questioned and deliberated in this manner, rather than analyzed quantitatively. As a rule, risks are quantitatively assessed only in classic gambling games (e.g., playing the odds at craps), in business and insurance decisions, and in some governmental regulatory actions.



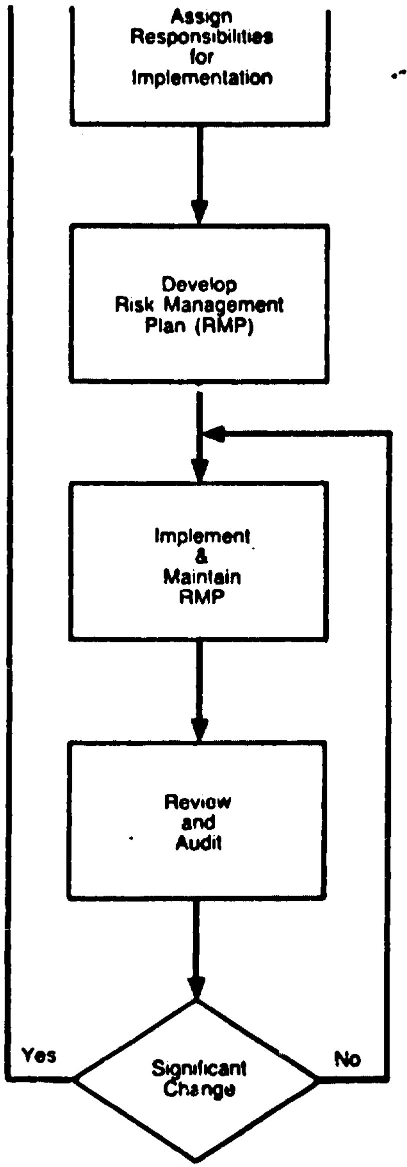
- Establishes Boundaries of Risk Environment
- Identifies Spec..c Risks Within Risk Categories
- Estimates Impact/Consequences of Risk Occurrence
- Identifies What Needs to Be Done

- Identifies What Controls Can Be Applied
- Identifies Cost of Controls (Implementation & Life Cycle Costs)

- Identifies Appropriate Controls
- Identifies Cost-Effective Controls
- Informs Management About Which Controls Should Be Applied

- Management Evaluation of Control Alternatives
- Management Determines Which Controls Will Be Applied

- Determines Who is Responsible for Implementing Controls


Assign Responsibilities for Implementation
Develop Risk Management Plan (RMP)
Implement & Maintain RMP
Review and Audit
Significant Change
Yes
No

- Determines Who is Responsible for Implementing Controls
- Identifies How Controls Will Be Implemented
- Establishes Time Frame in Which Controls Will Be Implemented
- Installation and Operation of Controls
- Determines How Well (Effectiveness) Controls are Working
- Identification of Changes and the Need to Evaluate Security Posture
- Decision to Conduct/Update Most Recent Risk Analysis/Review

FIGURE 2-1
THE ADP SECURITY RISK MANAGEMENT PROCESS

NEXT PAGE
BLANK

In the NASA ACP environment, quantifying risks is one of the necessary activities in determining which threats should be controlled.

### 2.1.1 Risk Definitions

Allen Willet in "The Economic Theory of Risk and Insurance" defines risk as "the objective uncertainty regarding the occurrence of an undesirable event." Frank Knight in "Risk, Uncertainty and Profit" defines risk as "measurable uncertainty." Derenburg, Eilers, Malone, and Zelten in "Risk and Insurance" define risk as "uncertainty of loss." All of these definitions involve some aspect of uncertainty.

Rowe states, "Uncertainty exists in the absence of information about past, present or future events, values, or conditions ... the basis of uncertainty is the absence of information about parts of a system under consideration." In the data processing environment, the process employed to reduce uncertainty is risk analysis.

## 2.2 Risk Analysis

Risk analysis attempts to answer the question, "What is at risk?" FIPS Pub 65, "Guidelines for Automatic Data Processing Risk Analysis," defines ADP security risk analysis as follows:

> The aim of risk analysis is to help ADP management strike an economic balance between the impact of risks and the cost of protective measures. It serves to point out the risks which exist; . . . An analysis shows the current security posture of ADP processing in an organization; it then assembles the basic facts necessary for the selection of adequate, cost effective safeguards.

A quantitative statement of risk is the result of two considerations: (1) the damage that can result from an unfavorable event, and (2) the likelihood that such an event will occur.

An analysis of risk involves the following procedures:

- Identify the scope of the risk environment and determine what is at risk.
- Identify the flaws in the environment that might permit the threats to materialize.
- Estimate the likelihood that the threats will occur.
- State the cost of loss that could be incurred if the threats to the risk environment were to materialize.

It should be understood that risk analysis, or the reduction of uncertainty, does not of itself reduce risk. Using the information gained from the risk analysis, a further analysis can be performed to determine what measures can be taken to reduce the identified risks and potential losses.

## 2.3 Risk Reduction Analysis

Risk reduction analysis can be viewed as an analytical process that attempts to answer the following questions: what controls are available to reduce risks, and which controls will provide the best security return on investment? The risk reduction analysis determines the cost of potential controls including both the implementation and maintenance costs. A cost-benefit analysis should be conducted to estimate the reduction in risk if the safeguards were to be applied. The final step in the risk reduction analysis is to recommend a set of controls to management. The recommendations should include a return o: investment calculation which provides a ratio of the expected loss reduction to the annual control cost.

## 2.4 Management Decisions

The choice and use of methods of treating risks are management decisions. In the government environment, management has four options for dealing with known risks:

1. Option 1 - Eliminate the Risk. The objective under this option is to eliminate vulnerabilities or potential vulnerabilities as early as possible in the system life cycle. At best this takes place early in the design and development of a system.

2. Option 2 - Loss Prevention. Controls should be implemented to prevent loss as far as possible when risks cannot be eliminated due to technological or operational reasons.

3. Option 3 - Loss Limitation. Loss limitation should be considered when prevention is not possible. The task of loss limitation is to limit the extent of loss to an acceptable level.

4. Option 4 - Accept the Risk. Management may decide to accept the risk and the consequences when the cost of loss is not significant, the cost to prevent or limit loss exceeds the potential loss, or the probability of loss is judged to be sufficiently small.

After the risk analysis and risk reduction analysis results are presented to management, decisions are made regarding the specific controls to be implemented. While the risk analysis team makes recommendations based on security need and return on investment, management should make the final selection based on its broader view of organizational mission, goals, and objectives. Management must designate priorities for the implementation of controls in consideration of other requirements for staff and budgetary resources, planned upgrades or replacement of equipment, planned major changes to existing systems and the developmental activities for new or replacement systems. Management should also make the initial determination regarding which organizational elements and/or personnel will be responsible for the implementation of controls and provide direction and guidance on the schedule for implementing those controls. In cases where the coordination or approval of other organizational and/or management personnel is required, management should assure that such coordination or approval is obtained. All decisions made by management concerning the risk analysis results should be documented for use by the risk management plan developers.

## 2.5 Development of Risk Reduction Action Plans

After management has determined which security controls will be implemented, the tasks leading to implementation must be accomplished. The risk reduction action plans must identify what controls are to be implemented, the systems and processes affected, the persons responsible, and the schedule for implementation. Depending on the type of control to be implemented, procurement activities may have to be initiated or internal design and development activities planned. Regardless of whether controls are procured from outside sources or developed internally, resources (personnel and money) will have to be obtained and allocated. In either case, the risk reduction action plan is the tool that will assure that security controls are implemented in a systematic manner.

## 2.6 Implementation and Maintenance of Controls

Implementation of security controls will necessitate some change in processes, functions, or responsibilities. Therefore, each person who is affected by any changes due to the implementation of controls must be convinced that: (1) there is a problem, (2) they can do something about it, and (3) it is advantageous to do so. Prior to implementing new controls, any changes in operations should be coordinated with affected personnel and additional training may also be required. Where possible, controls should be thoroughly tested to assure that they are operationally and technically sound. Once installed, controls should be maintained in accordance with the risk reduction action plans. When the risk environment changes, the maintenance process must be flexible enough to handle such changes.

## 2.7 Review and Audit

There should be a reasonable balance between the risk environment and the protection against such risks. Changes in operational processes, technology, and types of applications may result in materialization of new or different risks. Some risks may become less significant. Periodic reviews of security controls should be conducted to alert management to ineffective, non-functioning, or unneeded controls as well as indications of where new risks exist. Depending on the nature and magnitude of changes, an update to the previous risk analysis may be indicated.

Previous NASA guidance provided methodologies for conducting and documenting risk analysis and evaluating/certifying existing applications. The remainder of this document will provide guidance on an approach for assuring that the needed controls identified in risk analysis and application evaluation/certification are successfully implemented and maintained.

## 3. RISK MANAGEMENT PLAN DEVELOPMENT

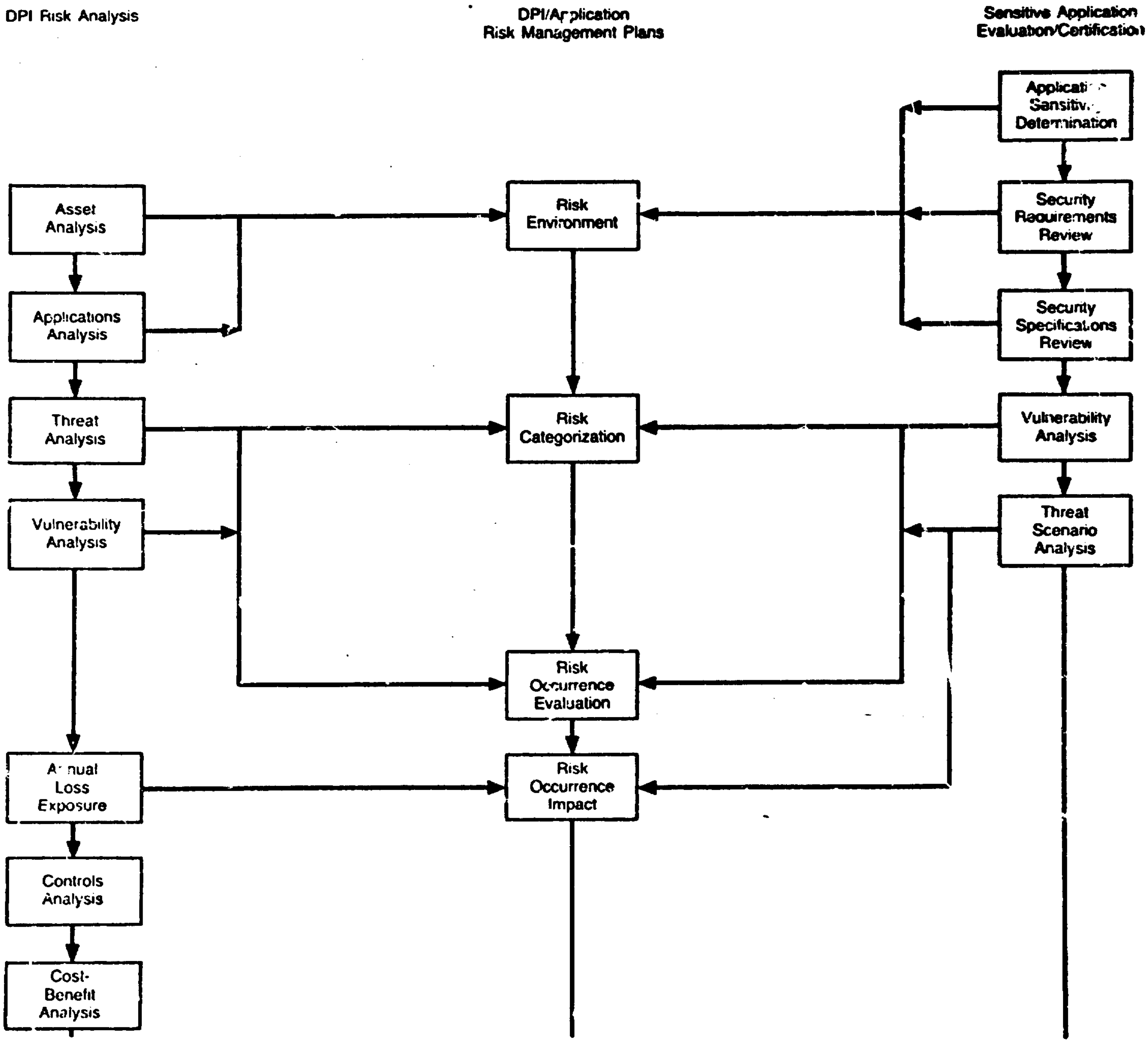
Appendix J, NHB 2410.1, states that sound management of risks demands documentation in the form of a risk management plan (RMP). The development of an RMP follows the conduct of a DPI risk analysis and/or a sensitive application evaluation/certification. An RMP includes a description of the risk environment, categorization of the risks to the risk environment, an evaluation of risk occurrence, the impact on the risk environment should the risks materialize, the degree to which risks can be controlled, and the actions which have been or are being taken to reduce risks. The development of an RMP will draw heavily upon the information that was collected or generated during the risk analysis or sensitive application evaluation. Separate guidance is provided for DPI and sensitive applications because separate methodologies are used within NASA to evaluate the risks to data processing installations and sensitive applications.

### 3.1 Preliminary Planning

As indicated previously, the guidance presented herein presumes that a risk analysis has been conducted at a data processing installation and/or an evaluation has been performed on an existing sensitive application. Although no reference is specifically made to new applications, it should be noted that (1) risk management plans should be developed for such applications and, (2) the development process described herein is sufficiently generic so that it can be employed by personnel developing RMP's for new applications. In addition to having accomplished a DPI risk analysis, the following guidance assumes that the risk analysis results have been presented to management and that management has made decisions regarding which risks will be accepted without additional controls being applied and which risks will be eliminated or reduced through the implementation of controls. Management decisions should include a projected time frame for implementation and designation of responsibilities for implementation. In the case of applications, management decisions and implementation guidance should be included in or be an outcome of the certification process. Figure 3-1 depicts the interrelationships between the major activities of a DPI risk analysis, an application evaluation/certification, and the risk management plan development process.

The analysis of assets and applications from the risk analysis provides the input for the risk environment section of the DPI RMP. The data for the sensitive application RMP should be found in the application sensitivity determination, security requirements review, and security specifications review portion of the application evaluation report. The threat and vulnerability analysis from the DPI risk analysis and the application system vulnerability analysis and threat scenario analysis provides the input to the risk categorization and risk occurrence evaluation sections of an RMP. The annual, loss-exposure phase of the risk analysis and the application threat scenario analysis provides the input for the risk occurrence impact portion of an RMP. The information required as input to the risk-reduction decision portion of the RMP are the risk analysis management decisions and the certification decisions concerning which controls will be implemented.

The risk-reduction action plans will primarily be based upon the management and certification decisions following a DPI risk analysis or an application evaluation/certification respectively.


DPI Risk Analysis
DPI/Application Risk Management Plans
Sensitive Application Evaluation/Certification
Application Sensitivity Determination
Asset Analysis
Risk Environment
Security Requirements Review
Applications Analysis
Security Specifications Review
Threat Analysis
Risk Categorization
Vulnerability Analysis
Vulnerability Analysis
Threat Scenario Analysis
Risk Occurrence Evaluation
Annual Loss Exposure
Risk Occurrence Impact
Controls Analysis
Cost-Benefit Analysis

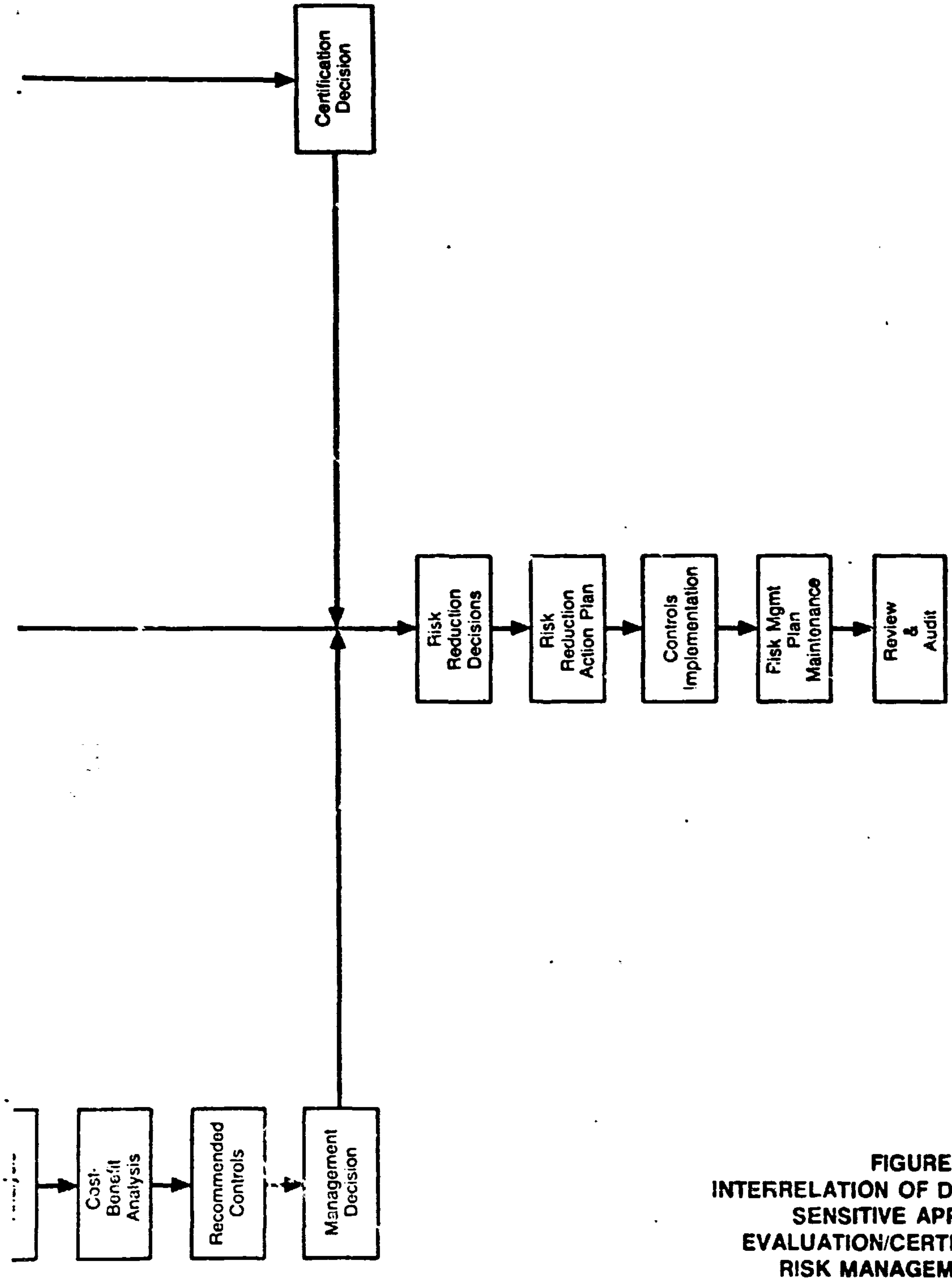


FIGURE 3-1
INTERRELATION OF DPI RISK ANALYSIS,
SENSITIVE APPLICATION
EVALUATION/CERTIFICATION AND
RISK MANAGEMENT PLANS

Additional data for design, development, or procurement planning may be required and will be discussed below. The next step is to develop an outline of the RMP. The development of DPI, applicatioc, and Center-level plans are discussed separately below.

### 3.2 DPI Risk Management Plans

The risk management plan for a data processing installation must be integrated with, and considered a part of, the DPI's computer security program. It should draw upon risk analysis documentation and not be a complete or substantial redocumentation of the risk analysis. Rather, the RMP should summarize the findings of the risk analysis and provide a road map for achieving a security posture in which risks are properly managed.

### 3.2.1 Risk Management Plan Framework

The risk management plan should be initially constructed in outline form siuilar to the sample provided in Appendix A. The major items should include: a description of the risk environment, risk categorization, risk occurrence evaluation, risk occurrence impact, risk reduction decisions, and risk reduction action plans.

### 3.2.2 Data Collection

The primary source of data for the risk environment, risk categorization, risk occurrence evaluation, and the risk occurrence impact is the risk analysis report and associated work papers. Additional sources of data for documenting the risk environment and risk categorization are the reports and

Preceding page blank

the supporting work papers of any internal audits, Inspector General reports, or management reviews. A list of personnel who were interviewed during the risk analysis and the names of management or operating staff who received briefings during the risk analysis should be compiled for use by the RMP developers. The RMP developers should also identify logistics and procurement personnel who can provide data and assistance for any controls that may involve procurement activities.

In the following discussions, references will be made to forms and worksheets utilized in the NASA Self-Analysis Guidance Document (SAGUD) for ADP Risk Analysis. Where appropriate, relevant forms or documentation from other methodologies should be utilized in developing RMPs.

### 3.2.3 Risk Environment

This section of the DPI risk management plan should provide a physical, organizational, and operational description of the data processing installation.

1. The physical description of the DPI should, at a minimum, include the following:

    a. Building number or name

    b. Physical location on the Center (street address or street boundaries)

    c. Brief description of the structure

    d. Room locations of computer hardware and peripherals

    e. Number and location of primary and emergency exits

    f. Location of user service areas or other public areas

g. Floor plan for each floor showing computer resource locations to include communications and major electrica˙ ⁿupport equipment

h. Description and location of physical security controls including guard stations, access control, alarms, and fire protection/suppression equipment

i. Storage areas for combustible supplies and media vaults

j. Descriptica of supporting utilities (e.g., power, air conditioning, etc.)

The above information may be obtained from Appendix B of the SACUD risk analysis report. The primary forms will be the Data Collectio Form and floor plans included or appended to the report.

2. The organizational description should include the following:

a. Copy of DPI mission statement

b. DPI functional organization chart with brief description of the units for both the NASA organization and facilities management contractor where appropriate

c. Key personnel telephone list

Organizational description data should be available from the risk analysis work papers and the Data Source Form found in Appendix B of the SACUD risk analysis report.

3. The operational description should include the following:

a. Listing of physical assets (e.g., computer hardware, peripherals, terminals, etc.)

b. Hardware configuration chart

c. Listing of vendor maintenance points of contact

d. Communications schematics

e. List of sensitive applications processed at DPI

f. Description of procedural and technical DPI controls (e.g., computer access controlled by a software security package that provides password protection to file level, etc.)

Operational description data should be found in Appendix B on the Asset Inventory Form.

If the above required data is not available from the SAGUD risk analysis report and attendant work papers, refer to Volume 1 of the Self Analysis Guidance Document, specifically Task 1, Step 3 ,and Task 2, Steps 1-8. Existing safeguards or controls are discussed in Chapters 3 and 5 of the SAGUD. Existing safeguards may also be found in the responses to the vulnerability questionnaire.

### 3.2.4 Risk Categorization

This section of the DPI risk management plan should identify the threats that may adversely impact the equipment, facilities, personnel, data, and supplies. Threats should be documented without reference to existing safeguards or controls designed to mitigate threats. The objective in documenting threats at this point in the plan is simply to provide an identification and to develop an understanding of the threats to the equipment, facilities, personnel, supplies, and data. The potential impact or consequences of any threat acting against the DPI will be documented in the risk occurrence impact section of the RMP.

Suggested ways of documenting th.eats include the following:

- Categorization by natural disasters, disasters of human origin, access problems, and system reliability hazards as discussed in NHB 2410, Appendix J, Section 503
- Threats by loss category; i.e., damage, denial of possession, denial of use and disclosure per SAGUD Volume II, Appendix C3, or as codified in Appendix C2
- Listing of threat definitions/scenarios as provided in Appendix E of this document

Threat data may be obtained from the Threat Asset Analysis Matrix form in Appendix B of the SAGUD risk analysis report.

### 3.2.5 Risk Occurrence Evaluation

Each threat should be evaluated with respect to its likelihood of occurrence. The nature of each threat will, in large part, determine the potential frequency of occurrence. In the case of natural disasters, geography, time of year, atmospheric patterns, etc., are major factors in estimating likelihood. In dealing with threats of human origin, likelihood of occurrence will be based, to a significant degree, on the reliability, integrity, and competency of personnel. The other major parameter affecting likelihood of occurrence will be the vulnerabilities of the DPI. Vulnerabilities may exist as a result of operational procedures, ineffective controls, or lack of controls. This section of the RMP should identify the threats, the vulnerabilities which would permit the threats to materialize, a statement of likelihood of occurrence, and an identification of existing controls assigned to reduce the occurrence rate. In those cases where likelihood of occurrence is based primarily on judgmental estimates rather than empirical evidence, the rationale for the estimate should be documented.

The primary sources of data for this section of the RMP are the Threat Asset Analysis Matrix, the Threat Asset Summary Form, and the Vulnerability Findings form from Appendix B of the SAGUD risk analysis report.

### 3.2.6 Risk Occurrence Impacts

The impact or consequences for each threat should be assessed. The impact is usually stated in monetary (dollar) terms and is determined by multiplying the single or one-time loss of an asset by the frequency of occurrence of each threat that may adversely affect the asset. Single-time loss for damage, denial of possession, denial of use and disclosure are usually determined separately. This section of the DPI risk management plan should identify each asset, the threats that may impact the asset, the vulnerabilities that would permit each threat to materialize, the annual frequency estimate for each threat, the single time loss, and the annual loss exposure. In those instances where the order of magnitude concepts were used due to difficulty in determining dollar values, a narrative description of the threat occurrence impact should be included.

The primary sources of data for this section of the RMP are the ALE Worksheets from Appendix B of the SAGUD risk analysis report.

### 3.2.7 Risk Reduction Decisions

The previous sections of the DPI risk management plan have involved extracting and/or summarizing data previously documented in the risk analysis report. The development of this section of the report is based on management's response to the risks identified and analyzed in the risk analysis and the control recommendations resulting from the risk reduction analysis.

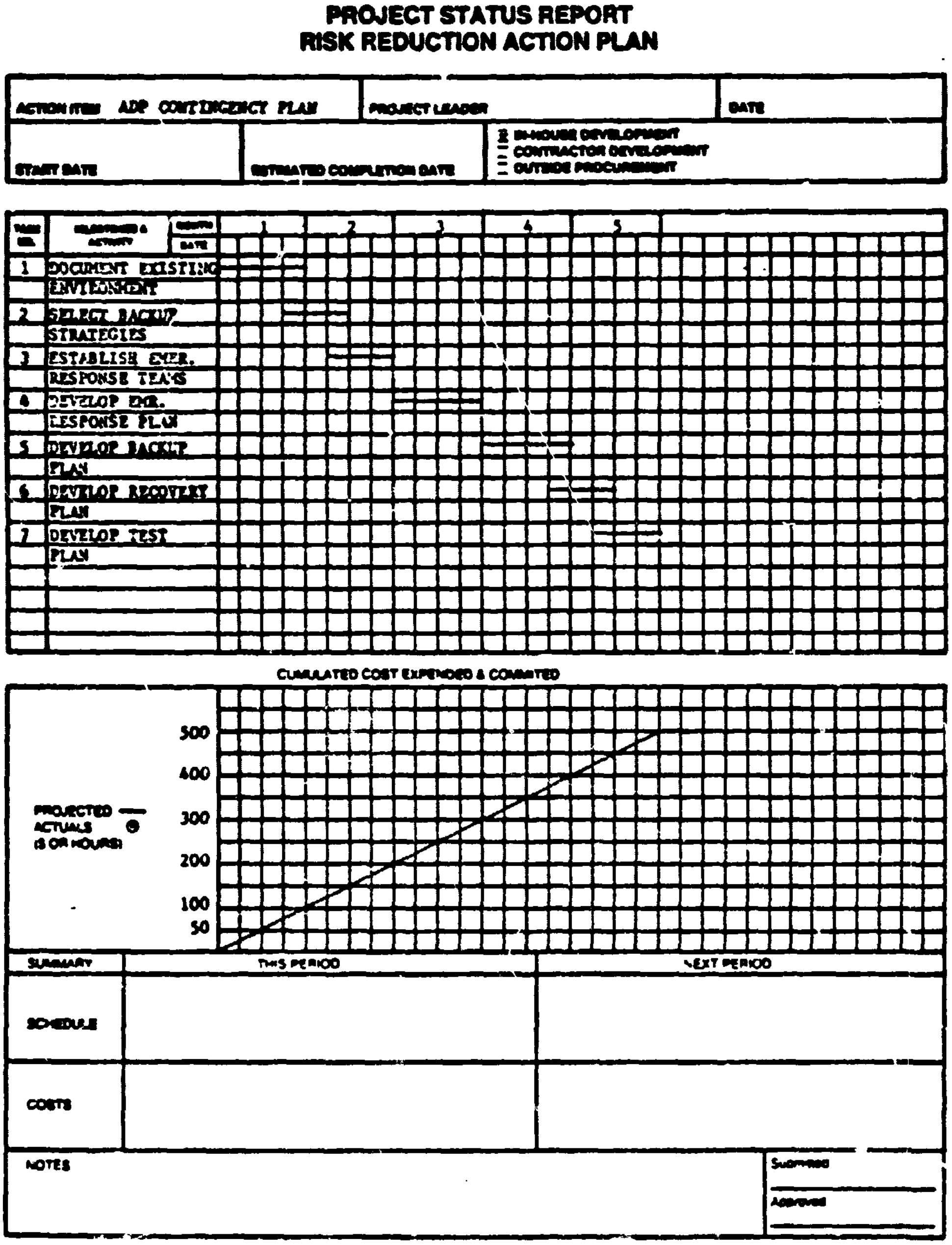
Each risk should be identified, the impact of risk occurrence on the organizational mission should be described, and the acceptability or nonacceptability of the risk should be indicated. For unacceptable risks, the controls currently in place as well as those approved by management for later implementation should be noted.

### 3.2.8 Risk Reduction Action Plans

Management's decisions should be turned into a set of action plans for implementing the needed controls. The data for the action plans should be contained in or attached to the decision paper originally provided to management. The action plans should provide detailed activities for the design, development, procurement, testing, and implementation of controls. At a minimum, it is recommended that a GANTT chart be developed indicating elapsed time to implmentation, with subtask schedules included. Project documents should permit the tracking of subtasks as well as resource expenditures. A sample risk reduction action plan for developing a contingency plan is shown in Figure 3-2.

## 3.3 Sensitive Application Risk Management Plans

The risk management plan for a sensitive application draws upon the data gathered and the analytical results documented during



PROJECT STATUS REPORT
RISK REDUCTION ACTION PLAN

| | | |
|---|---|---|
| ACTION ITEM ADP CONTINGENCY PLAN | PROJECT LEADER | DATE |

| | | |
|---|---|---|
| START DATE | ESTIMATED COMPLETION DATE | X IN-HOUSE DEVELOPMENT<br>_ CONTRACTOR DEVELOPMENT<br>_ OUTSIDE PROCUREMENT |

| TASK NO. | MILESTONES & ACTIVITY | MONTH 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 1 | DOCUMENT EXISTING ENVIRONMENT | | | | | |
| 2 | SELECT BACKUP STRATEGIES | | | | | |
| 3 | ESTABLISH EMER. RESPONSE TEAMS | | | | | |
| 4 | DEVELOP EMR. RESPONSE PLAN | | | | | |
| 5 | DEVELOP BACKUP PLAN | | | | | |
| 6 | DEVELOP RECOVERY PLAN | | | | | |
| 7 | DEVELOP TEST PLAN | | | | | |

CUMULATED COST EXPENDED & COMMITED

| SUMMARY | THIS PERIOD | NEXT PERIOD |
|---|---|---|
| SCHEDULE | | |
| COSTS | | |

NOTES

Submitted

Approved

FIGURE 3-2
PROJECT STATUS REPORT RISK REDUCTION ACTION PLAN

the evaluation/certification process. As in the case of a DPI RMP, the sensitive application RMP should, where possible, summarize the findings of the evaluation. The sensitive application RMP should provid^ a roadmap for achieving an unqualified certification of each sensitive application.

### 3.3.1 Risk Management Plan Framework

The risk management plan should be initially constructed in outline form similar to the outline sample shown in Appendix B. The major items to be included are: the application risk environment, risk categories, risk occurrence evaluation, risk occurrence impact, risk reduction decisions, and risk reduction action plans.

### 3.3.2 Data Collection

The primary source of data for the risk environment, risk categorization, risk occurrence evaluation, and the risk occurrence impact is the application evaluation report. Additional data may be gathered from system documentation, Audit and IG reports, and management reviews. Lists should be compiled of the personnel who were interviewed during the evaluation and also of the personnel who participated in the threat scenario analysis sessions. The risk management plan developer should identify the procurement personnel who are responsible for acquisition of ADP software and services.

In the following sections, references will be made to activities and forms utilized in the evaluation of existing sensitive applications, as described in "Guidelines for Certification of Existing Sensitive Applications" (MTR-82W0018). Relevant forms or documentation from other methodologies should be substituted in the development of RMPs as appropriate.

### 3.3.3 Risk Environment

This section of the sensitive application risk management plan should provide a general description of the application, the data, the security concerns, and the existing controls. The general description of the application should be available from Section 2 of the Evaluation Report. The general description of the application should, at a minimum, include the following:

- A functional overview of the application
- List of major users, data owners and data custodians, and the application CSO
- A description of the DPI that processes the application
- A description of the mode(s) of execution (i.e., batch, on-line, update, remote job entry, etc.)
- Identification of software package vendor (if appropriate) and a description of maintenance procedures
- A description of the sensitive or critical attributes of the application
- The type of data processed and generated by the application
- Description of any sensitive or critical processing algorithms
- List of other applications that utilize or require data from this application

The description of the security attributes should include the following:

- The data and system security objectives

- The security requirements and specifications

- Any existing security controls, including physical and technical safeguards and administrative procedures

### 3.3.4 Risk Categorization

This section of the sensitive application risk management plan should identify the threats that may adversely impact the integrity, confidentiality, or availability of the application and its associated data. Threats should be documented without regard to any existing or planned safeguards. The objective is simply to identify those events, situations, or personnel (by position) that have the capability to impact adversely the functions and data supported by the application. The potential impacts or consequences of any threat or threats acting against the application system as well as the effectiveness of any existing controls in mitigating these threats will be documented in the risk occurrence evaluation and impact sections of the RMP. The data for this section of the RMP should be extracted from the threat scenario analysis worksheet.

Suggested ways of documenting threats include:

- Categorization by threats to the application software (e.g., software development and maintenance, threats during program execution)

- Categorization of threats to data (e.g., during data preparation or entry, data base maintenance)

- Categorization of threats to output products (e.g., during distribution, storage or destruction operations)

- Listing of threats by security objective; i.e, integrity, confidentiality, availability, and deliberate or unintentional acts)
- Categorization by threats to security requirements

### 3.3.5 Risk Occurrence Evaluation

This section should document the likelihood that each threat or threat scenario will occur. Each threat or threat scenario should be listed, together with the vulnerabilities that would permit an attack to be mounted against the system, and a description of the controls that are in place to prevent or limit loss. The likelihood of threat occurrence should then be stated in high, medium, or low terms with an accompanying description of the rationale for this evaluation.

The primary source of data for this section of the report are the Threat Analysis Worksheets.

### 3.3.6 Risk Occurrence Impacts

This section of the report should state the monetary impact of a successful attack against the application and/or data. Where it is not possible or feasible to quantify the impact, a qualitative statement or narrative description of the consequences of a successful attack against the application and the associated data should be provided.

The primary source of data for this section of the RMP are the Threat Analysis Worksheets.

### 3.3.7 Risk Reduction Decision

The previous sections of the sensitive application risk management plan have involved the extraction and summarization of data from the sensitive application evaluation report. This section will be based upon the certification report provided to and the certification decision made by the application CSO. In this section of the RMP, each risk should be identified, the impact or consequences on the organizational missions should be described, and a notation should identify each risk as acceptable or not acceptable. For unacceptable risks, the controls currently in place as well as those approved by management for implementation should be noted.

### 3.3.8 Risk Reduction Action Plans

The successful implementation of additional safeguards for an existing application requires the development of one or more plans to provide control over design, development, procurement, and testing activities. The expenditure of dollar and personnel resources should also be monitored The data for the action plans should be contained in the supporting documents for the decision paper submitted, as appropriate, to the application CSO or upper managment. At a minimum, a simple GANTT chart should be prepared. This chart should indicate elapsed time for implementation and provide subtask schedules. A sample risk reduction action plan form is provided in Appendix F. (See Figure 3-2 for a completed example.)

### 3.4 NASA Center-Level Risk Management Plans

Center computer security officials should develop risk management plans that summarize ADP security risks across the entire Center. The primary objective of the Center-level risk management plan is to provide a management control process over DPI and sensitive application risk management plans. A secondary objective of the Center risk management plan is to provide the Center CSO with a mechanism to monitor the DPI and sensitive application risk management activities.

### 3.4.1 Risk Management Plan Framework

The Center-level risk management plan should be started in outline form similar to the sample provided in Appendix C. The major items in the outline should include: a description of the risk environment, risk categorization, risk occurrence evaluation, risk occurrence consequences, risk reduction decisions, and risk reduction action plans. It is recommended that separate subsections be established for DPI's and applications within each major section.

### 3.4.2 Data Collection

The primary sources of data for the Center risk management plan are the DPI and sensitive application risk management plans. The Center computer security official should also have access to Center-wide audits, IG reports, and management reviews.

### 3.4.3 Risk Environment

This section of the Center risk management plan should provide physical, organizational, and operational description of the Center's data processing environment. The physical description of the Center should include:

- Description of geographical location of the Center to include major metropolitan area(s) surrounding the Center

- Description of primary and secondary sources of electric power, telephone and other communications service, heating and cooling

- Physical location of utility distribution points at the Center

The organizational description of the Center should include the following:

- A Center mission statement

- A summary of the major type of activities conducted at the Center

- A functional organization chart that identifies major directorates at the Center

- A telephone listing of key management and operational personnel who have ADP and security responsibilities and also a telephone listing of DPI and sensitive application CSOs.

The operational description should include the following:

- Description of the open or closed nature of the Center (e.g., Center is open to visitors through Gate 1 during daylight hours with restricted access during hours of darkness)

- General description of Center security program such as the physical security procedures for employees, badge requirements, perimeter controls, etc.

### 3.4.3.1 Data Processing Installations

This portion of the risk environment section should include the following for each DPI:

- The location

- The primary functional uses (e.g., institutional data processing, mission control, etc.)

- A functional organization chart which identifies DPI managers

- The name and phone number of the DPI CSOs

- The date and major findings of the last DPI risk analysis

### 3.4.3.2 Sensitive Applications

This portion of the risk environment section should identify the sensitive applications processed at the Center. For each sensitive application the following items should be documented:

- The overall functional purpose of the application

- The DPI at which the application is processed

- The mode of execution (i.e., batch, on-line query, remote job entry)

- The type of data processed

- The name and telephone number of the application CSO and data owner

- The date of last evaluation and any qualification contained in the certification statement

### 3.4.4 Risk Categorization

This section of the Center risk management plan should identify the threats that may adversely affect Center-wide ADP operations. Threats should be listed in this section without regard to any existing or planned safeguards. For suggested ways of categorizing or listing threats refer to Sections 3.2.4

and 3.3.4 of this document. This section should be a summarization of the DPI and sensitive application risk categorization sections.

### 3.4.5 Risk Occurrence Evaluation

Each Center-wide threat should be evaluated with respect to likelihood of occurrence. This section of the Center risk management plan should identify each threat, the vulnerabilities that might permit the threat to materialize, the controls or safeguards designed to reduce the likelihood of occurrence, and a statement indicating likelihood of occurrence. In those instances where likelihood of occurrence is primarily based on judgmental estimates rather than empirical evidence, the rationale for the estimate should be documented. Again, this section should be built on corresponding sections in the DPI and sensitive application RMPs.

### 3.4.6 Risk Occurrence Impacts

The impact or consequences for each threat should be assessed. The impact should be stated in dollar terms. Consequences should be stated in qualitative terms. At the Center-level, most impacts to Center-wide ADP operations should be described in terms of consequences. Detailed statements of impact are not recommended for the Center-level risk management because the impact on each DPI or application will be contained in individual DPI and application RMP's which should be available to the Center CSO.

### 3.4.7 Risk Reduction Decisions

This section of Center-level risk management plan should summarize the management's ADP security program decisions. It should indicate the guidance that management has provided for reducing ADP secur'ty risks at the Center-level. For example, a Center manageme . decision to have all DPIs conduct an initial risk analysis within the next two years would be included in this section of a Center RMP.

### 3.4.8 Risk Reduction Action Plans

Management's decisions concerning Center-wide ADP security risks should be turned into a set of action plans. Each action plan should identify the major task and subtasks, the estimated and elapsed time to completion, the responsible person, and the estimated and actual resource expenditures. It is suggested that a GANTT chart be developed similar to the example in Figure 3-2.

## 3.5 Integration of DPI and Sensitive Application Risk Management Plans

In some NASA environments, it may be desirable to integrate the DPI and sensitive application risk management plans into a single document. This would apply in a case where a single sensitive application is the only application processed on a stand-alone micro or mini computer. Integration of plans may also be appropriate where ADP security risk management responsibilities for both the DPI and a sensitive application are assigned to a single computer security official. Separation of DPI and sensitive application specific data should be maintained in the RMP sections addressing the risk environment, risk categorization, risk occurrence evaluation, and risk occurrence impact. However, integration of the risk reduction action plans is appropriate where one individual is responsible for managing the risks associated with both the DPI and the sensitive application.

### 3.6 Coordination of DPI and Sensitive Application Risk Management Plans

Although the above guidance has made a distinction between DPI and sensitive application risk management plans, it is obvious that computer facilities and applications are interdependent. It is, therefore, important to maintain close liaison between the personnel who develop and maintain DPI and sensitive application risk managment plans. Coordination of risk reduction action plans is of special concern where the measures required to reduce the risks in an application system are dependent upon technical features inherent to the computer hardware or the operating system software.

### 3.7 Sensitivity of Risk Management Plans

Risk managment plans, like risk analysis reports, provide a consolidated statement of the security posture of a data processing installation or a sensitive application. The information contained in the RMP is extremely valuable to personnel whose interests and objectives are inimical to those of NASA. Therefore, the number of copies of risk management plans and any associated work papers should be limited. The distribution of copies should be tightly controlled. Copies should not be left on shelves or desk tops unattended.

## 4. RISK MANAGEMENT PLAN MAINTENANCE

The maintenance of risk management plans should be focused on three major areas:

1. Monitoring of risk reduction actions plans to ensure that the design, development, procurement and implementation of controls proceed according to schedule and within budget
2. Auditing of implemented controls to determine their effectiveness
3. Reviewing physical, organizational and operational activities to identify changes that might necessitate re-evaluation or modification of current risk reduction measures

### 4.1 Monitoring of Risk Reduction Action Plans

The actions preceding the implementation of some controls may closely parallel a system acquisition life cycle. For example, procurement and installation of an access control software package may involve several months of procurement activities, several months of developing access rules or matrices, training, testing, and phased implementation. Some controls, such as an ADP contingency plan for a major computer facility, will require as much as six months to a year for the development phase. Therefore, risk reduction action plans must be continually monitored to ensure that schedules are adhered to as closely as possible and that deviations from the schedule are reasonable and approved by management. It is also important to ensure that management is periodically informed on the progress of the action items. Normal project control procedures should be used for monitoring risk reduction action plans.

## 4.2 Audit of Implemented Controls

The primary purpose of auditing implemented controls is to determine their effectiveness. It should be remembered that if a control is totally effective, the specific risk being protected probably will not materialize. Similarly, if the vulnerability being mitigated by control has not been exploited, the risk may not materialize. Controls must be audited to ensure that they operate as designed. Controls should be periodically tested. Documented procedures for using the control should be reviewed to ensure that they are being followed. As part of an effectivess audit, controls should be evaluated to determine if the control has created a more serious vulnerability or risk than it was designed to reduce.

## 4.3 Reviewing Physical, Organizational and Operational Activities

A risk management plan is a management tool that must be able to respond to changes in the physical, organizational, and operational environment. Changes to physical facilities, the introduction of a new computer system, implementation of new systems, and promulgation of new regulations may affect the risk environment. New risks may appear and some risks may disappear, thus negating the requirement for some controls or establishing a requirement to modify existing controls. Organizational changes may result in changes of responsibility for control implementation and maintenance activities. Additionally, control technology is constantly advancing which may reduce the cost of controls which were not previously considered to be cost-effective.

All of the foregoing changes should be monitored by risk management plan developers. In those instances where a change is considered significant, modifying current controls should be evaluated against the need to update the most recent DPI risk analysis or sensitive application evaluation. Furthermore, the development and implementation of risk management principles, techniques, and tools in the data processing environment will be a new experience for many NASA personnel. As experience is gained, progressive interaction of risk management plans and of these guidelines will be required.

# APPENDIX A

## OUTLINE FOR DPI RISK MANAGEMENT PLAN

1. INTRODUCTION

   1.1 Purpose
   1.2 Background

2. RISK ENVIRONMENT

   2.1 Physical Description
   2.2 Organization Description
   2.3 Operational Description

3. RISK CATEGORIZATION

   3.1 Damage Threats
   3.2 Denial of Possession Threats
   3.3 Denial of Use Threats
   3.4 Disclosure Threats

4. RISK OCCURRENCE EVALUATION

   4.1 Damage Threats
   4.2 Denial of Possession Threats
   4.3 Denial of Use Threats
   4.4 Disclosure Threats

5. RISK OCCURRENCY IMPACTS

   5.1 Impact/Consequences of Damage Threats
   5.2 Impact/Consequences of Denial of Possession Threats
   5.3 Impact/Consequences of Denial of Use Threats
   5.4 Impact/Consequences of Disclosure Threats

6. RISK REDUCTION DECISIONS

   6.1 Acceptable Risks
   6.2 Unacceptable Risks

7. RISK REDUCTION ACTION PLANS

   7.1 Project Plan for Risk Reduction Action Item 1
   7.2 Project Plan for Risk Reduction Action Item 2

## APPENDIX B

## OUTLINE FOR
## SENSITIVE APPLICATION RISK MANAGEMENT PLAN

1. INTRODUCTION

    1.1 Purpose
    1.2 Background

2. RISK ENVIRONMENT

    2.1 General Description
        2.1.1 Functional Overview
        2.1.2 Users, Owners, Custodians, CSO
        2.1.3 Description of Hardware Support
        2.1.4 Type of Data Processed
        2.1.5 Sensitive/Critical Attributes
        2.1.6 Sensitive/Critical Algorithms
        2.1.7 Associated Application Systems
    2.2 Security Attributes
        2.2.1 Data and System Security Objectives
        2.2.2 Security Requirements
        2.2.3 Security Specifications
        2.2.4 Existing Controls

3. RISK CATEGORIZATION

    3.1 Integrity Threats
    3.2 Confidentiality Threats
    3.3 Availability Threats
    3.4 Fraud Threats

4. RISK OCCURRENCE EVALUATION

    4.1 Integrity Threats
    4.2 Confidentiality Threats
    4.3 Availability Threats
    4.4 Fraud Threats

5. RISK OCCURRENCE IMPACTS

    5.1 Impact/Consequences of Integrity Threats
    5.2 Impact/Consequences of Confidentiality Threats
    5.3 Impact/Consequences of Availability Threats
    5.4 Impact/Consequences of Fraud Threats

6. RISK REDUCTION DECISIONS

6.1 Acceptable Risks
6.2 Unacceptable Risks

7. RISK REDUCTION ACTION PLANS

7.1 Risk Reduction Action Item 1
7.2 Risk Reduction Action Item 2
7.3 Risk Reduction Action Item 3

# APPENDIX C

## OUTLINE FOR
## NASA CENTER
## RISK MANAGEMENT PLAN

1. INTRODUCTION

1.1 Purpose
1.2 Background

2. RISK ENVIRONMENT

2.1 Physical Description of Center
2.2 Organizational Description of Center
2.3 Operational Description of Center
2.4 Data Processing Installations
2.4.1 DPI Locations
2.4.2 DPI Functions
2.4.3 DPI Orgnization
2.4.4 DPI CSO
2.4.5 Date and Major Findings of Last DPI Risk Analysis
2.5 Sensitive Applications
2.5.1 Functional Overview of Applications
2.5.2 Supporting DPI
2.5.3 Type of Data Processed
2.5.4 Application CSO and Data Owner
2.5.5 Date of Last Evaluation and Qualifications to Certification

3. RISK CATEGORIZATION

3.1 Threats to Data Processing Installations
3.1.1 Damage Threats
3.1.2 Denial of Possession Threats
3.1.3 Denial of Use Threats
3.1.4 Disclosure Threats
3.2 Threats to Sensitive Applications
3.2.1 Integrity Threats
3.2.2 Confidentiality Threats
3.2.3 Availability Threats
3.2.4 Fraud Threats

4. RISK OCCURRENCE EVALUATION

4.1 Threats to Data Processing Installations
4.1.1 Damage Threats
4.1.2 Denial of Possession Threats
4.1.3 Denial of Use Threats
4.1.4 Disclosure Threats
4.2 Threats to Sensitive Applications
4.2.1 Integrity Threats
4.2.2 Confidentiality Threats
4.2.3 Availability Threats
4.2.4 Fraud Threats

5. RISK OCCURRENCE CONSEQUENCES

5.1 Threats to Data Porcessing Installations
5.1.1 Consequences of Damage Threats
5.1.2 Consequences of Denial of Possession Threats
5.1.3 Consequences of Denial of Use Threats
5.1.4 Consequences of Disclosure Threats.
5.2 Threats to Security
5.2.1 Consequences of Integrity Threats
5.2.2 Consequences of Confidentiality Threats
5.2.3 Consequences of Availability Threats
5.2.4 Consequences of Fraud Threats

6. RISK REDUCTION DECISIONS

6.1 Acceptable Risks
6.2 Unacceptable Risks

7. RISK REDUCTION ACTION PLANS

7.1 Risk Reduction Action Item 1
7.2 Risk Reduction Action Item 2
7.3 Risk Reduction Action Item 3

# APPENDIX D

## BIBLIOGRAPHY

Army, Department of the, Automated Systems Security, Army Regulation 380-380, October 14, 1977

Derenburg, Herbert S., et al, Risk and Insurance, 2nd ed., Prentice-Hall, 1974.

Garrison, H.G. Jr., and Simpson, G.A., An Overview of ADP Risk Analysis, MTR-79W00445, The MITRE Corporation, November 1979.

Giragosian, P. A., Mastbrook, D. W. and Tompkins, F.G., Guidelines for Certification of Existing Sensitive Systems, MTR-82W00018, The MITRE Corporation, July 1982.

Knight, Frank, Risk, Uncertainty and Profit, Haughton Mifflin, 1971.

NASA Handbook (NHB) 2410.1, Computer Resources Management.

NASA Management Instruction (NMI) 2410.7, Assuring Security and Integrity of NASA Data Processing.

National Bureau of Standards, FIPS PUB 31 - Guidelines for Automatic Data Processing Physical Security and Risk Management, June 1974.

National Bureau of Standards, FIPS PUB 65 - Guidelines for Automatic Data Processing Risk Analysis, August 1, 1979.

National Bureau of Standards, FIPS PUB 73 - Guidelines for Security of Computer Applications, June 30, 1982.

Office of Management and Budget, Security of Federal Automated Information Systems, Circular A-71, Transmittal Memorandum No. 1, July 27, 1978.

"Risk Management," Security Management, American Society for Industrial Security, pgs 16-21, May 1977.

Rowe, William D., An Anatomy of Risk, John Wiley and Sons, Inc. 1977.

Self Analysis Guidance Document for Conducting NASA Risk Analysis (Draft), EDP Audit Controls, Inc., March 1982.

Smith, James E., "Risk Management for Small Computer Installations," *Advances in Computer Security Management*, Heyden & Son, Inc., 1977.

Tompkins, F.G., *Risk Analysis: A Tool Not a Solution*, Third Annual Seminar on Security of Federal Automated Information Systems, Federal ADP Users Group, June 3, 1982.

Transportation, Department of, Federal Aviation Administration, *FAA Computer Risk Assessment Handbook* (Draft), FAA Order 1600.XX, August 1980.

Willit, Allen, *The Economic Theory of Risk and Insurance*, University of Pennsylvania Press, 1951.

# APPENDIX E

## THREAT DEFINITIONS

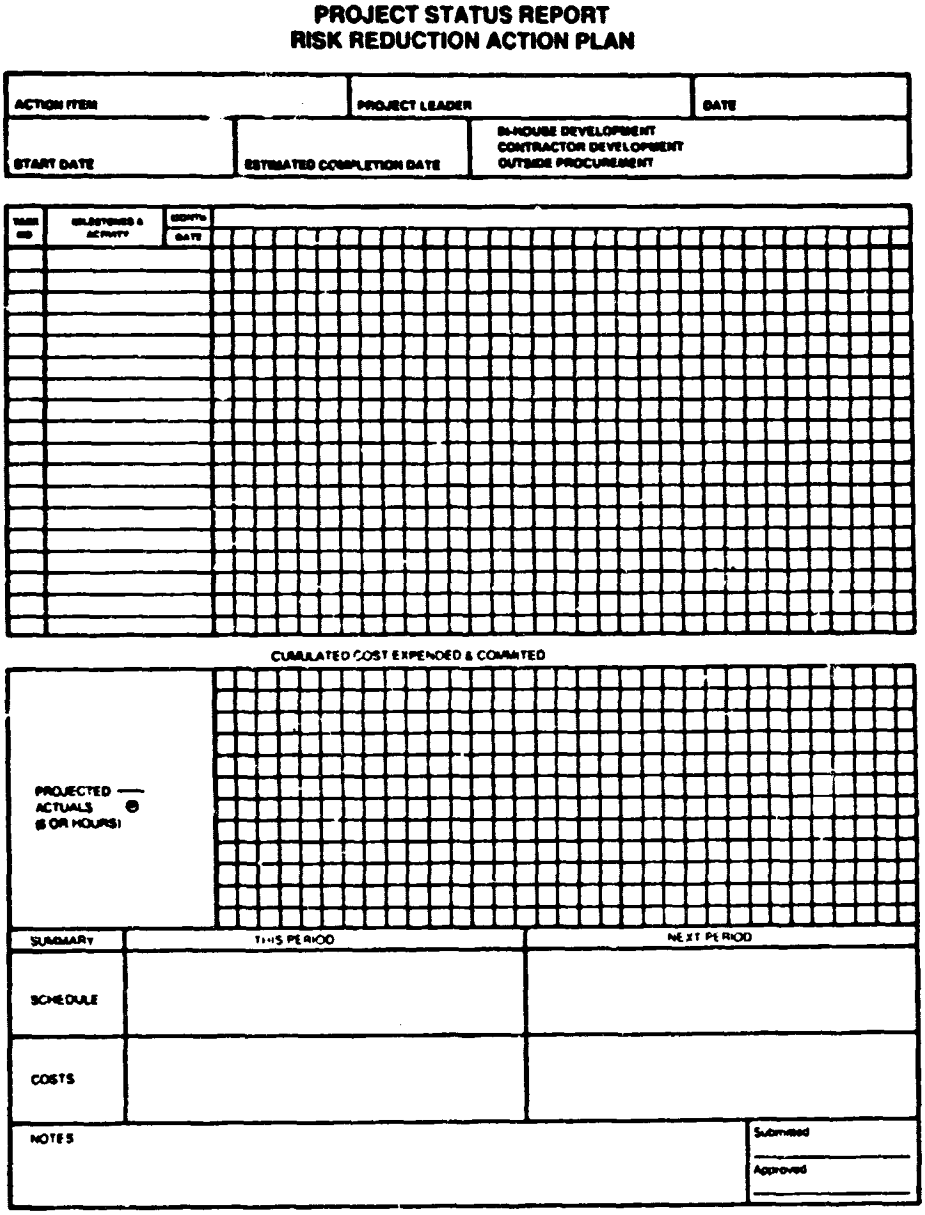
| THREAT | DEFINITION/SCENARIO | EXAMPLE |
|---|---|---|
| VANDALISM | Opportunistic destruction of property (major level is considered sabotage). | Breaking a window |
| THEFT | Pilferage of available equipment conveyable by one person. | A stolen terminal |
| CIVIL DISORDER | An outside group blocks access to gates and facilities. | Anti-government protest |
| LABOR DISPUTE | An inside group disrupts access to facilities. | Programmer's strike |
| BOMB THREAT | A telephone bomb threat that is taken seriously, facility is evacuated. | Typical bomb threat |
| ARSON/BOMBING | Fire or explosion for purposes of personal emotional satisfaction. | Pyromaniac employee |
| TERRORISM INCIDENT | Occupation of a facility by a hostile group, with damage. | Hostage situation |
| SABOTAGE, OUTSIDERS | Professional sabotage aimed at disrupting U.S. space program, max. damage. | Blow up power station |
| SABOTAGE, MAJOR | Organized attack on major equipment, labor related scenario. | Destroy CPU |
| SABOTAGE, MINOR | Organized minor damage to equipment, labor related scenario. | Coke in terminals |
| WATER LEAKAGE | Plumbing leak or ruptured roof, including accidental sprinkler discharge. | Water pipe break |
| AIR CONDITIONING | Disruption of cooling utility service to an ADP area. | Air handler failure |
| POWER FLUCTUATION | Momentary disturbance to electrical power affecting ADP operations. | Crash due to voltage drop |
| BROWNOUT | Extended reduction of electrical power affecting ADP operations. | Power reduction |
| BLACKOUT | Extended loss of electrical power to facility or zones. | Transfomer failure |
| COMM. DISRUPTION | Short term disruption of external telecommunications. | Noise on phone lines |

| THREAT | DEFINITION/SCENARIO | EXAMPLE |
|---|---|---|
| ACCIDENTAL EXPLOSION | Zone dependent, equipment arcing/explosion, chemical explosion, etc. | CRT implosion |
| FIRE, MINOR | Small fire confined to one piece of equipment or a small area. | Fire in tape drive |
| FIRE, MAJOR | Fire in a major equipment or impacting "major" level of zone assets. | CPU burnout |
| FIRE, CATASTROPHIC | Total destruction of exposure zone assets by fire. | Burnout of computer room |
| FLOOD | Flooding due to creek/river overflow, not hurricane related. | "100 year level" flood |
| SEVERE STORM | Winds less then 100 mph, hail, ice, lightning, tropical storms. | Violent thunderstorm |
| HURRICANE | Nominal level hurricane, winds about 120 mph, no storm surge. | Major exterior damage |
| TORNADO | Direct tornado impact on ADP facility or great hurricane and storm surge. | Total destruction |
| SUBSIDENCE FAULTING | Ground faulting due to subsidence differentials. | Utility tunnel cracks |
| EARTHQUAKE | Minor earth tremors, Richter magnitude of less than 5.0 assumed. | Minor building shake |
| HUMAN ERROR | Accidental acts by persons. | Operator mismounts tape |
| SYSTEM RELIABILITY | Unavailability of hardware (computer) due to system failure. | System crash |
| COMP. SYSTEM ABUSE | Unauthorized use of computer system resources. | Illegal file on system |
| INSIDER | A person allowed working access to facilities. | NASA employee/contractor |
| OUTSIDER | A person not allowed working access to facilities. | General public/visitor |

## APPENDIX F

## PROJECT STATUS REPORT
## RISK REDUCTION ACTION PLAN

NEXT PAGE
BLANK



PROJECT STATUS REPORT
RISK REDUCTION ACTION PLAN

ACTION ITEM

PROJECT LEADER

DATE

START DATE

ESTIMATED COMPLETION DATE

IN-HOUSE DEVELOPMENT
CONTRACTOR DEVELOPMENT
OUTSIDE PROCUREMENT

TASK NO

MILESTONES & ACTIVITY

MONTH

DATE

CUMULATED COST EXPENDED & COMMITED

PROJECTED —
ACTUALS ⊖
($ OR HOURS)

| SUMMARY | THIS PERIOD | NEXT PERIOD |
|---|---|---|
| SCHEDULE | | |
| COSTS | | |

NOTES

Submitted

Approved

Preceding page blank