DOT/FAA/AR-99/94

Office of Aviation Research
Washington, D.C. 20591

FAA WJH Technical Center
00021440

Guide to the FAATC Risk Management Process

COPY 3

Richard T. Lazarick

Aviation Security Research and Development Division
Federal Aviation Administration
William J. Hughes Technical Center
Atlantic City International Airport, NJ 08405

ATION ADMINISTRATION
JUL 2 4
TECHNICAL CENTER LIBRARY
ATLANTIC CITY INT'L AIRPORT, NJ 08405

June 1999

This report is approved for public release and is on file at the William J. Hughes Technical Center, Aviation Security Research and Development Library, Atlantic City International Airport, NJ 08405

This document is available to the public through the National Technical Information Service (NTIS), Springfield, Virginia 22161

U.S. Department of Transportation
Federal Aviation Administration

DOT/FAA
AR-99/94
C. 3

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No. DOT/FAA/AR-99/94	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle GUIDE TO THE FAATC RISK MANAGEMENT PROCESS		5. Report Date June 1999
		6. Performing Organization Code AAR-510
7. Author(s) Richard T. Lazarick		8. Performing Organization Report No.
9. Performing Organization Name and Address U.S. Department of Transportation Federal Aviation Administration William J. Hughes Technical Center Aviation Security Research and Development Division Atlantic City International Airport, NJ 08405		10. Work Unit No.
		11. Contract or Grant No. DT059-96-D-00410
12. Sponsoring Agency Name and Address U.S. Department of Transportation Federal Aviation Administration Associate Administrator for Civil Aviation Security, ACS-1 800 Independence Avenue, S.W. Washington, DC 20590		13. Type of Report and Period Covered Final Report
		14. Sponsoring Agency Code ACS-1

15. Supplementary Notes

Report Prepared by:

Monica S. Grusche
Abacus Technology Corporation
5454 Wisconsin Avenue, Suite 1100
Chevy Chase, MD 20815

DOT/FAA AR-99/94
Guide to the FAATC risk management process
C. 3
00021440
Tech Center Library

16. Abstract

This report provides a summary and guidance to the Federal Aviation Administration (FAA) William J. Hughes Technical Center (FAATC) Risk Management Process, developed by Abacus Technology Corporation in conjunction with the FAATC. Abacus Technology used the Risk Management Process in conducting risk/vulnerability assessments of airports in support of the FAA Airport Vulnerability Assessment and Analysis Project (AVAP). The report includes a discussion of risk management concepts; a summary of the process modeling approach used to diagram the process steps; a description of the process; a complete diagram of the process; and a glossary of terms and concepts.

17. KEY WORDS Risk Assessment; Risk Analysis; Vulnerability Assessment; Vulnerability Analysis; Automated Tool; Vulnerability; Threat; Countermeasures; Physical Security.		18. Distribution Statement This document is available to the public through the National Technical Information Service (NTIS), Springfield, Virginia 22161	
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 75	22. Price

Form DOT F1700.7 (8-72) Reproduction of completed page authorized

This page intentionally left blank.

TABLE OF CONTENTS

Page

1. INTRODUCTION 1
   1.1 Background 1
      1.1.1 Airport Security Risk Assessment R&D 1
      1.1.2 Airport Security Risk and Vulnerability Assessment 2
   1.2 Objective 3
   1.3 Scope 3
2. APPROACH TO RISK MANAGEMENT 4
   2.1 Discussion of Concepts 4
   2.2 Methods of Estimating Risk 5
   2.3 Qualitative vs. Quantitative Risk Assessment 6
3. PROCESS MODELING APPROACH 7
   3.1 Theory and Structure of an IDEF0 Model 7
      3.1.1 The Node Index 8
      3.1.2 The Context Diagram 8
      3.1.3 Activity Diagrams with Accompanying Text 9
      3.1.4 The Glossary 9
      3.1.5 IDEF Model Decomposition 10
   3.2 IDEF0 Representation of the Risk Management Process 10
4. RISK MANAGEMENT PROCESS 11
   4.1 Establish Risk Management Strategic Plan [A1] 13
   4.2 Formulate Approach [A2] 14
      4.2.1 Define Scope [A21] 15
      4.2.2 Define Boundary [A22] 16
      4.2.3 Determine Analysis Approach and Tools [A23] 17
      4.2.4 Plan Project [A24] 18
   4.3 Assess Risk [A3] 19
      4.3.1 Collect Data [A31] 20
         4.3.1.1 Collect Asset Information [A311] 21
         4.3.1.2 Collect Threat Information [A312] 24
         4.3.1.3 Collect Countermeasure Information [A313] 26
      4.3.2 Evaluate Vulnerability [A32] 28
      4.3.3 Evaluate Risk [A33] 29
   4.4 Select and Implement Countermeasures [A4] 30
   4.5 Monitor Countermeasure Effectiveness and Changes in Risk Factors [A5] 32
5. BIBLIOGRAPHY 33

TABLE OF CONTENTS (CONTINUED)

Page

APPENDIX A: THE FAA WILLIAM J. HUGHES TECHNICAL CENTER RISK MANAGEMENT PROCESS A-1

APPENDIX B: GLOSSARY OF TERMS AND CONCEPTS B-1

TABLE OF FIGURES

Page

Figure 1. Visual Representation of the Scope of an Analysis 4
Figure 2. Examples of Relative Scales of Measurement 5
Figure 3. IDEF0 Representation of an Activity 9
Figure 4. IDEF0 Decomposition Structure 10
Figure 5. Airport Security Risk Management 11
Figure 6. Establish Risk Management Strategic Plan 13
Figure 7. Formulate Approach 14
Figure 8. Define Scope 15
Figure 9. Determine Analysis Approach and Tools 17
Figure 10. Plan Project 18
Figure 11. Assess Risk 19
Figure 12. Collect Data 20
Figure 13. Collect Asset Information 21
Figure 14. Determine and Prioritize Critical Assets 22
Figure 15. Determine Asset Value 23
Figure 16. Collect Threat Information 24
Figure 17. Develop Perpetrator Profile 25
Figure 18. Collect Countermeasure Information 26
Figure 19. Characterize Countermeasures 27
Figure 20. Evaluate Vulnerability 28
Figure 21. Select and Implement Countermeasures 31
Figure 22. Monitor Countermeasure Effectiveness and Changes in Risk Factors 32

1. INTRODUCTION

The Federal Aviation Administration, William J. Hughes Technical Center (FAATC), has designed and developed a complete process for managing security risk at the nation's airports. This guide provides an overview and quick reference for the approach, concepts, and definitions involved in the FAATC Risk Management Process and a description of the process itself.

1.1 Background

This report is one of a series of investigative and analytical reports to document the results of the research conducted in association with the development of the Risk Management Process. Since 1992, Abacus Technology Corporation has been supporting the FAATC Airport Security Program. The primary objective of the Airport Security Program is to provide a structured technology framework for administering the research, development, and integration of all components of the civil aviation security system. Software, hardware, training, procedures, human factors, airport design, and the National Airspace System (NAS) design are integrated by the program to provide a total civil aviation security system which provides the maximum protection with the least risk and operational impact.

A key responsibility of the FAA is to plan for and set policy to provide a safe and secure aviation system for the flying public. A prime method for setting security goals is to use a vulnerability assessment and risk management process to prioritize security objectives and evaluate alternatives. The FAATC Aviation Security Research and Development Division has defined the requirement to design, develop, implement, and test a vulnerability assessment and risk management process for airport security. From this requirement, a project to develop a vulnerability assessment and risk management process was created.

1.1.1 Airport Security Risk Assessment R&D

In September 1996, Abacus Technology began assisting the FAATC in their objective to develop an airport security risk and vulnerability assessment process. This research and development (R&D) effort resulted in several associated, interim reports:

a. The *Functional Methodology for Risk Management*

b. An *Evaluation of the Security Analysis Support System (SASSy) Customized for Civil Aviation Security*, and

c. An *Assessment of Airport Security Environment.*

The report that initiated the Risk Management Process R&D effort was an evaluation of risk and vulnerability methodologies currently in use in various industries. A search, comparative review, and evaluation of existing of risk analysis methodologies was conducted. The resulting report, FAATC Technical Report DOT/FAA/AR-96/1, *Functional Methodology for Risk Management*, December 1996, provides a description of the issues surrounding the airport environment, reviews risk/vulnerability assessment requirements in various industries, postulates a risk management functional methodology for airports, and presents an R&D approach to accomplishing the risk process development.

In connection with the then ongoing investigation and evaluation of risk and vulnerability assessment methodologies expected to be applicable for meeting airport security requirements, FAATC requested that Abacus Technology conduct an independent review of the Security Analysis Support System (SASSy). SASSy, an automated risk analysis and survey tool, was customized for aviation security under contract to the FAA Office of the Associate Administrator for Civil Aviation Security (ACS). Aviation-customized SASSy was evaluated against its established application development goals, against the needs of ACS and of the FAA Civil Aviation Security Field Offices (CASFOs), and against FAA's airport and facility security requirements. The findings are presented in FAATC Technical Report DOT/FAA/AR-97/1, *Evaluation of the Security Analysis Support System (SASSy) Customized for Civil Aviation Security*, January 1997.

The FAATC analyzed the security environment at U.S. airports to serve as a starting point from which the process of defining, quantifying, and analyzing airport vulnerabilities and risks. The goal was to establish a baseline of the current conditions at U.S. airports with regard to security issues, describe existing assets common to various categories and configurations of airports, and establish a baseline description of typical airports. This analysis is documented in FAATC Technical Report DOT/FAA/AR-97, *Assessment of Airport Security Environment*, August 1997.

1.1.2 Airport Security Risk and Vulnerability Assessment

In October 1997, independent events provided the FAATC and Abacus Technology the opportunity to test the Risk Management Process at operational U.S. airports. The FAATC established the Airport Vulnerability Assessment Project (AVAP) in response of the White House Commission on Aviation Safety and Security recommendation to conduct periodic vulnerability assessments of the nation's commercial airports. The FAATC tasked Abacus Technology with conducting vulnerability assessments at two U.S. airports in support of the AVAP. Abacus Technology applied the Risk Management Process in conducting the assessments. The application of the Risk Management Process in the AVAP is documented in three of the project reports:

a. The Airport Vulnerability Assessment Master Plan
b. The *Denver International Airport (DEN) Vulnerability Assessment Report*, and
c. The *Detroit Metropolitan-Wayne County Airport (DTW) Vulnerability Assessment Report*.

The *Airport Vulnerability Assessment Master Plan*, December 1997, defined the overall approach that Abacus Technology employed in conducting airport risk and vulnerability assessments in support of the AVAP. The methodology used was a combined qualitative and quantitative approach using the Risk Management Process. The *Denver International Airport (DEN) Vulnerability Assessment Report*, September 1998, and the *Detroit Metropolitan-Wayne County Airport (DTW) Vulnerability Assessment Report*, September 1998, present the results of Abacus Technology's risk and vulnerability assessments.

1.2 Objective

The objective of this guide is to present the overall Risk Management Process developed through the FAATC R&D efforts. The Risk Management Process that emerged is a flexible, comprehensive process for managing risk that can be applied to other environments as well as airport security. The Process encompasses risk management activities from establishing a strategic plan to assessing and mitigating risk to monitoring the risk environment. The intent of this guide is to provide an overview and quick reference for the approach, concepts, and definitions involved in the FAATC Risk Management Process and guidance to conducting risk management activities in any environment.

1.3 Scope

This guide is divided into two functional segments. The first half describes risk concepts fundamental to understanding the Risk Management Process (Section 2) and the Integration DEFinition Language 0 (IDEF0) process modeling approach taken to developing the Process (Section 3). The second half of the guide describes the complete Risk Management Process (Section 4). Two appendices to this guide are intended to provide quick reference to using the Process. Appendix A presents the entire IDEF0 diagram of the Risk Management Process. Appendix B is a glossary of risk terms and a cross-reference to Risk Management Process steps.

2. APPROACH TO RISK MANAGEMENT

Risk management goes beyond a single risk assessment and includes: monitoring changes in the environment, exploring new security procedures and technologies, and periodically recommending cost-effective security countermeasures that provide the best protection available within the budget provided. The process discussed below is a complete and thorough definition of the entire risk assessment and management process.

2.1 Discussion of Concepts

A risk assessment is specific to the system being analyzed; therefore, before undertaking a risk assessment, it is important to have an understanding of the system and its setting. Figure 1, and the corresponding definitions and discussion below it, illustrate the concepts involved in the risk assessment process.

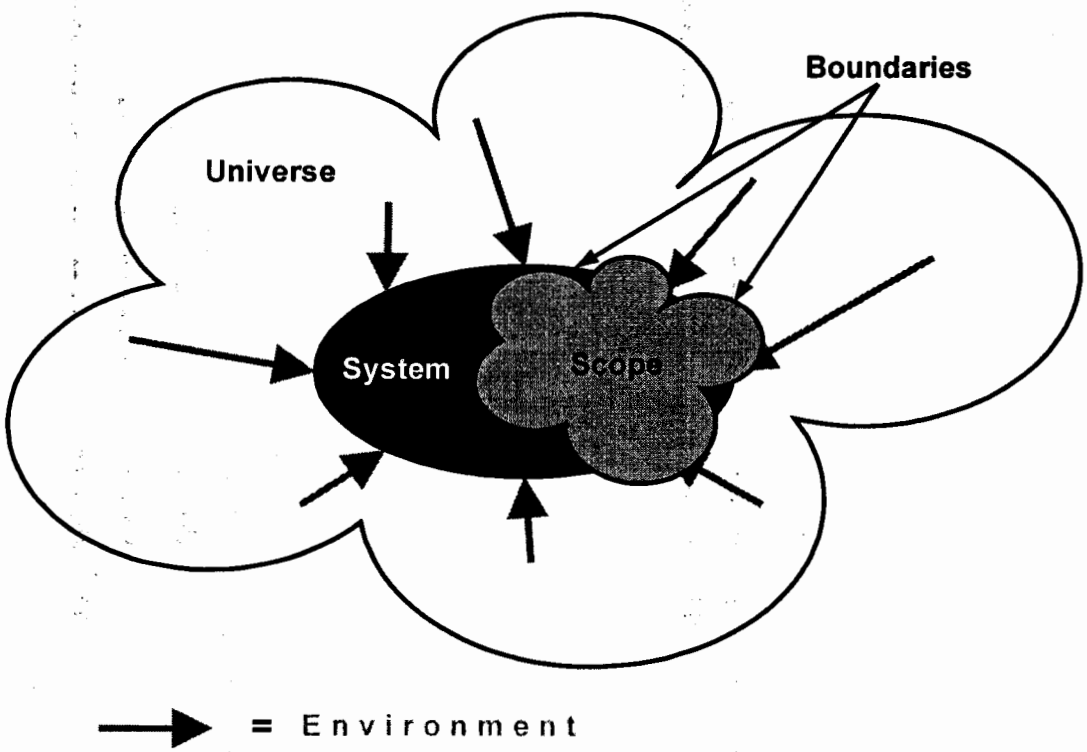


Figure 1. Visual Representation of the Scope of an Analysis

Universe – All existing systems and conditions.

System – A group of interrelated, interacting, or interdependent components in the universe forming a complex whole to accomplish a mission.

Environment – The external circumstances, conditions, and characteristics that affect the existence and development of the system.

Boundary – The border or limit of the system defined in the scope.

Scope – The delineation of level of effort, areas of the universe, and boundaries of the systems that are covered in the risk assessment process.

A ***system*** is an organization and all of its physical components, assembled to accomplish a particular mission. The system exists as part of the ***universe*** of all possible systems. Depending on the size and complexity of a system, it is composed of any number of subsystems. The system's ***boundary*** defines the extent of the system in question. A system does not exist in isolation. External forces act upon the system and can influence its behavior. These external forces, such as weather, location, or condition of the local economy, comprise the system's ***environment*** and can affect the system's ability to accomplish its mission. The ***scope*** of a risk assessment distinguishes the system being analyzed, and includes characteristics of the environment and other aspects of the universe deemed relevant to the analysis task at hand.

2.2 Methods of Estimating Risk

Risk is an abstract concept that can be measured on two types of scales—relative and absolute. Relative scales do not have standards of comparison, i.e., they are a means of ranking risk values in relation to other values on the same scale. Since relative values are not based on a firm standard, they can have distinct meanings depending on the user and the context. A common example of a relative scale for expressing risk is a Low/Medium/High scale. Figure 2, below, shows how two Low/Medium/High scales can correspond to different ranges of values composed on a linear scale.

Figure 2. Examples of Relative Scales of Measurement

Another type of relative scale for risk measurement is the specification of a range of values, for example, a scale of 1 to 10 or percentages from 1% to 100%. Using numerical values such as these as representative values does not change the relative structure of the scales. The values of risk are still defined in relation to each other.

Absolute scales, on the other hand, are scientific measuring systems (e.g., English and Metric systems) which quantify many aspects of physical space and time. The standards on which they are based are documented by organizations like the National Institute of Standards and Technology (NIST). Their existence allows us to consistently compare objects and duration. An example of an absolute measurement of risk is annual loss expectancy (ALE). Another is the probability of intercepting (P_i) an aggressor who is attempting to carry out a threat against the system. P_i is based on the event timings that exist for a particular physical layout and a specific set of paths that the threat may exploit and may be expressed as a single number or a distribution.

2.3 Qualitative vs. Quantitative Risk Assessment

Whereas relative and absolute scales are methods of expressing risk analysis inputs and results, the terms -- qualitative and quantitative -- describe approaches to risk assessment. A qualitative risk assessment is a "top-down" technique. It starts with a definition of an ideal (standard) for comparison. The standard is typically a set of best practices, suggested or mandated, defined by expert judgment and/or derived from previous risk analyses, including quantitative analysis. A qualitative risk assessment focuses on the possible countermeasures for the system. For example, vulnerabilities in a qualitative assessment are defined by what the current system lacks as compared to the standard.

The inherent assumption in qualitative risk assessment is that the protection level of the current system would be improved if it more closely matched the standard. The primary limitation to a qualitative risk assessment approach is that it directly depends upon how well the ideal is defined. An advantage of a qualitative assessment is that it can be conducted very quickly.
A quantitative risk assessment is a representation of the current system from a "bottom up" perspective. That is, a quantitative risk assessment starts with a mathematical (i.e., fault-tree) or graphical-path model of the physical, operational, and procedural layout of the current system. The goal of a quantitative risk assessment is to represent the current system as accurately as possible and then analyze its behavior. Analysts use the scientific method of investigation and test theories in order to replicate the behavior of the real world. As in a qualitative risk assessment, the scope of the system still must be defined. For instance, some assumptions may be made up front as to the range of threats considered in the model. Since no judgments are made regarding the performance of the system in developing a quantitative model, the quantitative approach is best suited to uncover weaknesses in the system that may be counter-intuitive or otherwise go unrecognized. Quantitative methods include probabilistic and simulation modeling techniques.

3. PROCESS MODELING APPROACH

Some important definitions must be introduced at this time: processes, process steps, and methods (or methodologies). A *process* is a repeatable, well defined and tested set of procedures for accomplishing a complex task. The manufacturing industry is notable for its requirement to accurately define and develop specific processes. In that industry, processes are developed and implemented to build a specific product. The process is first engineered (options analyzed, methods formulated) and then defined in detailed process specifications. The resulting processes are the proprietary, often patented, secrets that give one firm a competitive advantage over another.

The process is made up of many *process steps*. Process steps are discrete and highly defined actions (by machines or people or both) that accomplish the specific step. Continuing with a manufacturing example, each step has an input, such as a blank sheet of metal, and a desired output, such as stamped shapes or cuts. Each step may also have associated constraints such as specific materials requirements. The step may define specific controls, such as restrictions on the amount of pressure the metal will bear. Each process step output will be the input to another process step until the product is complete.

In each step of the process, various methodologies may have been evaluated prior to final process specification (e.g., pressing the metal part from sheet metal stock with a 10-ton press versus creating a mold and forming the part from molten metal). These various methods may all achieve the same goal – the final product – but some methods may be much less expensive, more reliable, or easier to accomplish given the resources available.

3.1 Theory and Structure of an IDEF0 Model

In this report, a particular method for representing processes will be used: the IDEF0 (Integration DEFinition Language 0) approach. IDEF0 is a process modeling methodology used to model a variety of automated and non-automated systems. The original IDEF0 program objective was to provide increased productivity for manufacturing through the rigorous application of computer technology. IDEF0 is intuitive because it is consistent with three fundamental facts about the way in which people process information within our culture, that is, IDEF0:

a. Handles graphic and text information from left to right and top to bottom

b. Uses visual placement to convey the type of information or importance of an activity, and

c. Captures a wealth of information graphically--a picture is worth a thousand words.

IDEF0 enables the documentation of processes and systems for reengineering purposes. In developing new systems, IDEF0 can be used to define the requirements and functions of a process and then to design an implementation process that meets the requirements and accomplishes the functions. For existing systems, IDEF0 can be used to analyze system functions and record the means by which the functions are carried out.[1] For the purposes of this report, IDEF0 will be used both to define existing risk assessment/management processes and to define a new risk management approach that is appropriate to an airport environment. The airport risk management approach will be modeled using IDEF0 and based on airport requirements and *best practices* of the risk assessment/management approaches reviewed. An IDEF0 model is a complete, concise, and consistent description of the activities or processes of a system or subject area. The model is developed from a particular viewpoint for a particular purpose. Each model consists of four main parts: (1) a node index, (2) a context diagram, (3) a set of activity diagrams with accompanying text, and (4) a glossary. The following is a brief introduction to the IDEF0 modeling technique.

3.1.1 The Node Index

The node index is an indented listing showing nodes in an IDEF0 model in "outline" order. The node index provides both a written system summary and a way to rapidly identify particular system activities.

3.1.2 The Context Diagram

The context diagram (A-0 Page) establishes the scope and purpose of the process as well as the particular viewpoint. It identifies the system boundaries (interfaces) with the outside world. Everything in the model comes from a decomposition of the context diagram.

[1] National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication (FIPS PUB) 183, *Integration Definition for Function Modeling (IDEF0)*, Dec. 21, 1993.

3.1.3 Activity Diagrams with Accompanying Text

The diagrams and accompanying text descriptions of the process define the model. The activity diagram is the basic work unit in modeling. It is primarily a box with arrows. The boxes represent activities of the system being modeled. Boxes (activities) are labeled with verbs or verb phrases and are defined in the narrative section of the model. Arrows connect boxes and represent interfaces or interconnections between the boxes. Arrows may split (branch) or join more than one activity. In the IDEF0 analysis method, each side of a box has a specific meaning. The left side is reserved for inputs (things that are transformed into outputs by the activity) and the right side is reserved for outputs (transformed inputs). The top is reserved for controls (constraints or rules that dictate the conditions of the transformation) and the bottom side is reserved for mechanisms (tools, people, and systems that are used during the transformation). Inputs, controls, outputs, and mechanisms are referred to using the acronym ICOM. Each ICOM is labeled and defined in the glossary section of the model (see Figure 3).

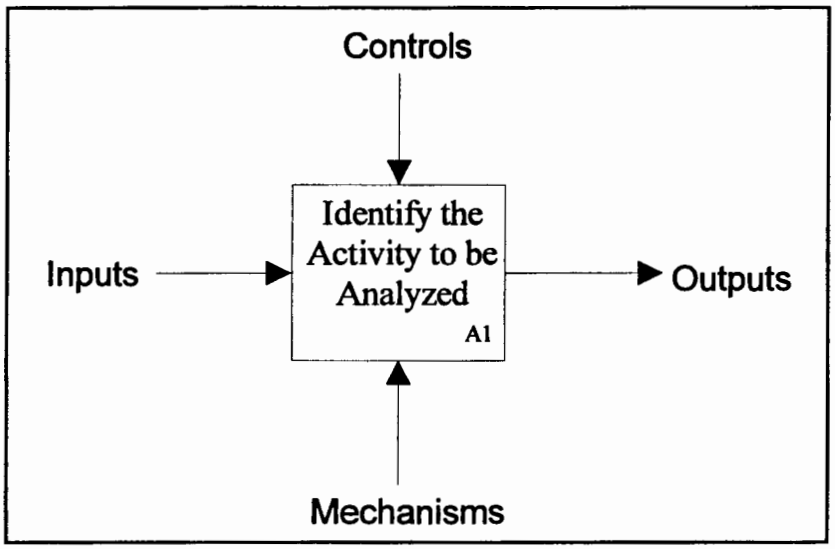


Figure 3. IDEF0 Representation of an Activity

3.1.4 The Glossary

Glossary entries define the technical words, phrases, synonyms, and acronyms used with a particular project. These definitions expand understanding of the terms appearing in the diagram and thus permit briefer box and arrow labels, which make diagrams easier to read and understand.

3.1.5 IDEF Model Decomposition

IDEF0 models show a top-down decomposition from the Context Diagram. The first level of decomposition breaks the context diagram (A-0) into three to six subordinate activities (boxes). The title for each diagram is taken verbatim from the box it decomposes. The result is a model whose top diagram describes a system in broad general terms, and whose bottom diagrams provide very detailed descriptions of the system activities, as shown in Figure 4.

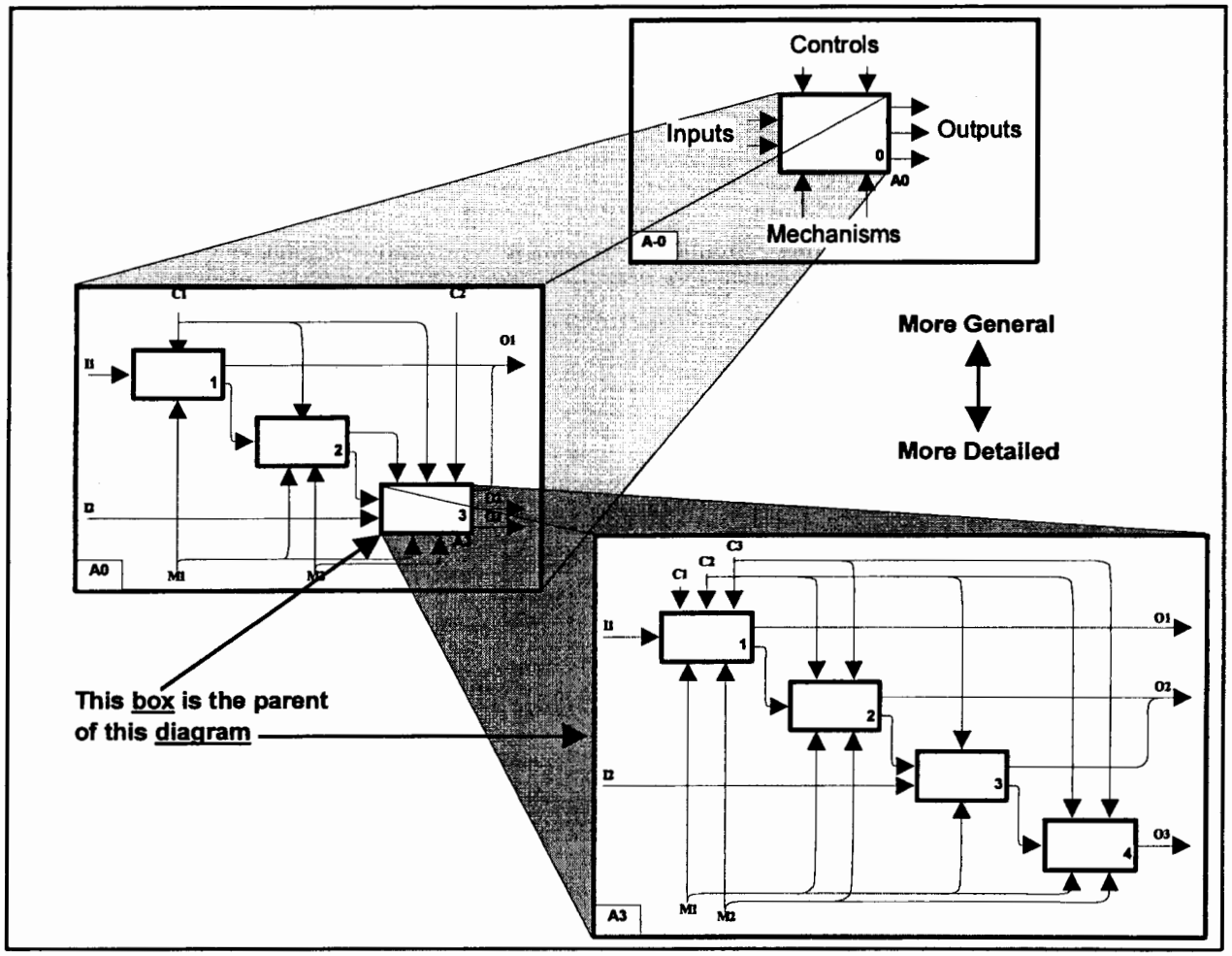


Figure 4. IDEF0 Decomposition Structure

3.2 IDEF0 Representation of the Risk Management Process

Using the IDEF0 methodology, the FAATC has designed and developed a complete process for managing the security risk at the nation's airports. It outlines, in detail, the specific steps that need to be taken in any vulnerability assessment, risk analysis, or risk management project. The highly structured and refined process for security planning, project definition, risk analysis, countermeasure selection, and ongoing risk monitoring is discussed in the following section.

4. RISK MANAGEMENT PROCESS

Risk management encompasses all aspects of vulnerability and risk assessments and defines management constraints which limit the potential options available for making trade-offs. Risk management includes defining a basic security strategy, budget constraints, and high-level policy decisions on the acceptable levels of residual risk. It also includes methods for updating the risk assessment over time to adjust to new threats or changes in assets. The primary objectives in the airport risk management process development are to:

a. Quantify the performance of existing and planned protective measures

b. Provide sufficient vulnerability and countermeasure trade-off information for security managers to modify existing or establish new security policies, and

c. Suggest a method for monitoring and control of the risk situation as the environment and technology change over time.

This section presents a generalized, flexible and comprehensive process description of a generic risk management process applied to airport security. The process, modeled using IDEF0 techniques, starts with a strategic plan and ends with steps to monitor and improve the resulting risk posture of the airport. Risk management also encompasses procedures to perform *what-if* studies and re-evaluations (and therefore, redesigns) of the security system over time. An overview of the resulting airport risk management process is provided in Figure 5.

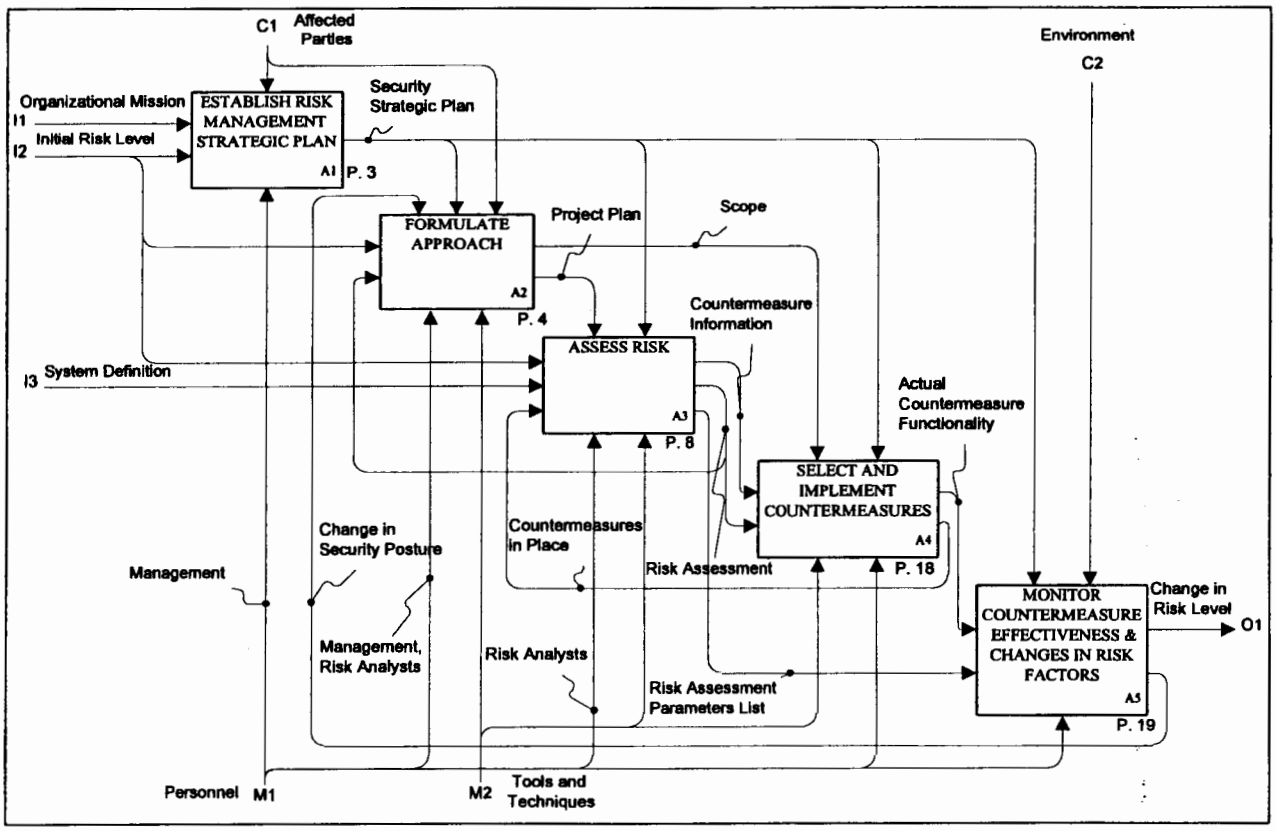


Figure 5. Airport Security Risk Management

In the following sections, each component of the proposed process will be discussed in the context of the first-level activity (A1 through A5) that they support:

a. Establish Risk Management Strategic Plan (A1);
b. Formulate Approach (A2);
c. Assess Risk (A3);
d. Select and Implement Countermeasures (A4); and
e. Monitor Countermeasure Effectiveness and Changes in Risk Factors (A5).

To better understand the process flow, standard IDEF0 terminology will be used to refer to the level of detail (Node) being discussed. The decomposition of an activity will be depicted on a separate page of the IDEF0 diagram, titled and numbered according to its parent. For example, the decomposition of the activity box [A1], *Establish Risk Management Strategic Plan,* will be shown in a separate figure titled *Establish Risk Management Strategic Plan* with Node [A1]. Each of the activity boxes on the A1 page will be numbered consecutively by adding a digit to the end of the Node number, for example, A11, A12, A13, and so on. This numbering scheme is similar to that of an outline format. The entire IDEF0 process definition can also be depicted like an outline or *Node Tree* (refer to Appendix A, pages A-24 and A-25, for the Node Tree of the Risk Management Process). Note that the Node Tree for the IDEF0 diagram described in Section 4 of this document also corresponds to its heading numbering. The complete IDEF0 diagram for the functional risk management methodology is shown in Appendix A.

4.1 Establish Risk Management Strategic Plan [A1]

The risk management process begins with the step Establish Risk Management Strategic Plan as shown in Figure 6. The decomposition of establishing a risk management strategic plan consists of establishing objectives (Establish Objectives, A11), policy (Establish Policy, A12), and authority and coordination (Establish Authority and Coordination, A13). The essential input is knowledge of the specific system's environment, specifically the organization's mission and the initial risk level of the system.

Using an airport security system as an example, complex environmental aspects need to be addressed. Airports are public facilities that attract very large numbers of citizens (and non-citizens) and therefore present a unique set of security issues. The basic mission of the airport is to safely and efficiently board and deplane passengers. To achieve its mission, the personnel involved in protecting and managing the airport must formulate long term, strategic objectives for security. Existing regulations and security policy must be organized in such a way as to create solid, manageable security procedures and lay out clear lines of responsibility and authority for the various organizations involved in security. The coordinated efforts of the responsible parties should produce a high level strategic security plan which will guide the efforts of all groups involved in the production of a usable risk assessment.

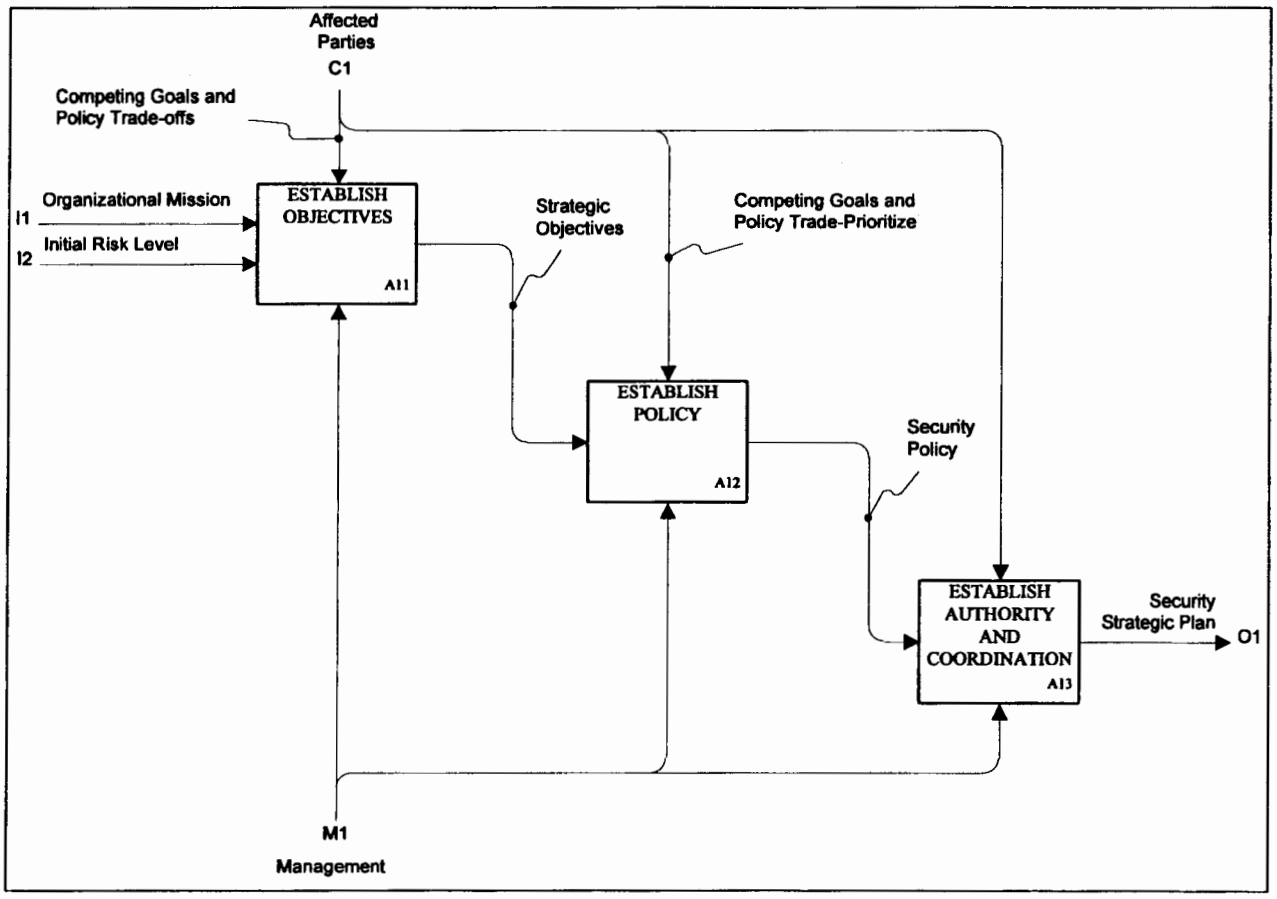


Figure 6. Establish Risk Management Strategic Plan

4.2 Formulate Approach [A2]

In any investigation, a clear definition of what is being analyzed is essential. Managing risk may affect diverse organizations over an extended period of time. To properly coordinate the efforts of the various groups involved and ensure that each process step is leading towards a common goal, it is necessary to formulate an approach (Formulate Approach, A2) that clearly defines the scope (Define Scope, A21) and boundary (Define Boundary, A22) of the system, select the analysis approach and tools (Determine Analysis Approach and Tools, A23) that will be utilized during the risk assessment process, and plan the project (Plan Project, A24). The process steps for the activity Formulate Approach (A2) are presented in Figure 7. The activities which constitute formulating the approach (A21 – A24) are discussed in detail in Sections 4.2.1 – 4.2.4.

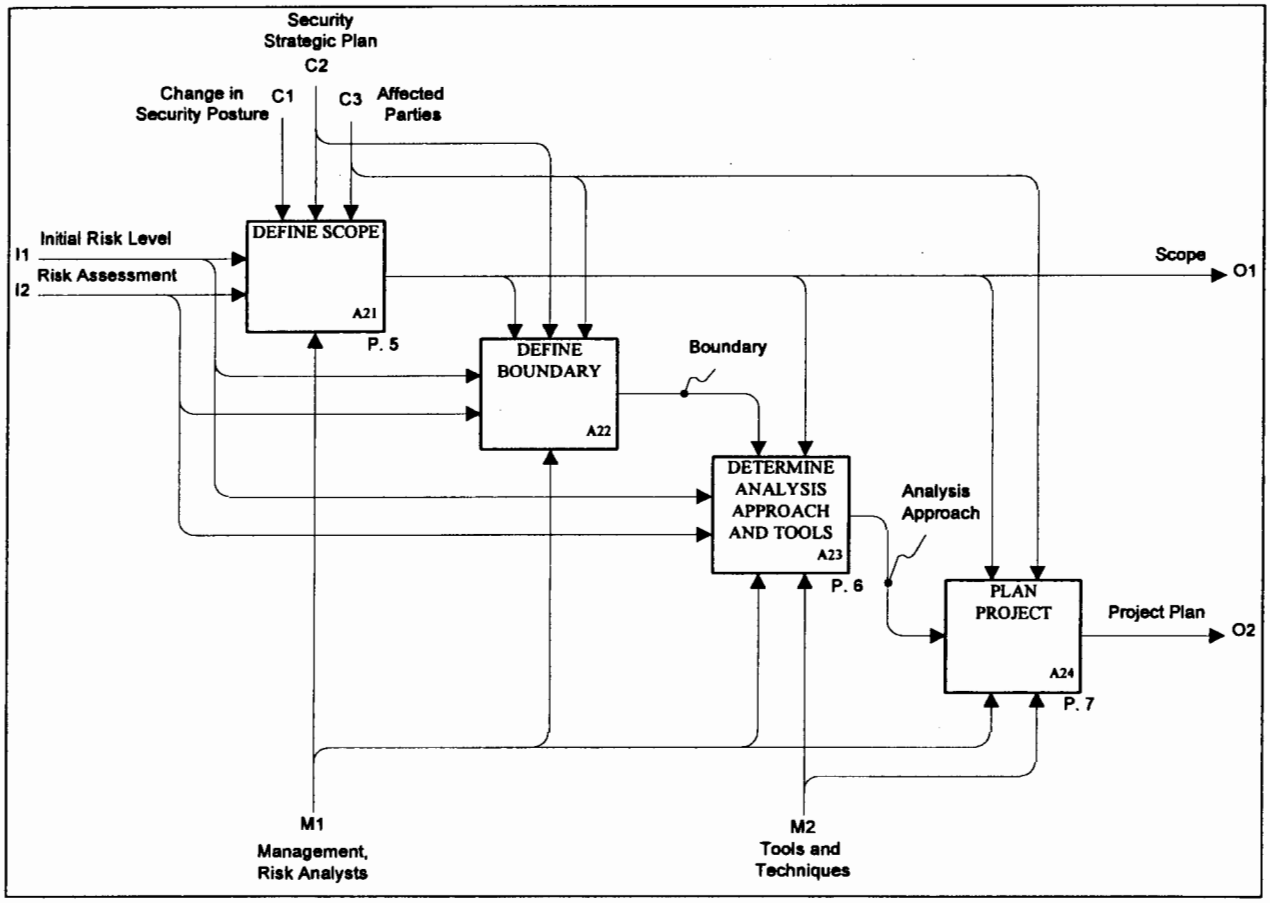


Figure 7. Formulate Approach

4.2.1 Define Scope [A21]

Scope is best thought of as *level of effort* and *breath of objectives* (Refer to Section 2.1 for a definition and explanation of *scope*). In certain instances, a top-level view of essential issues effecting risk may be all that is necessary. The level of effort may involve only a few key personnel with the objective of resolving only one security issue. Likewise, a comprehensive risk management study involving an analysis of all current threats to aviation, affecting all critical airport assets, and new countermeasure technologies may be very labor and time-intensive (even with the use of automated tools to assist in the process). The process steps for Define Scope (A21) are shown in Figure 8, below.

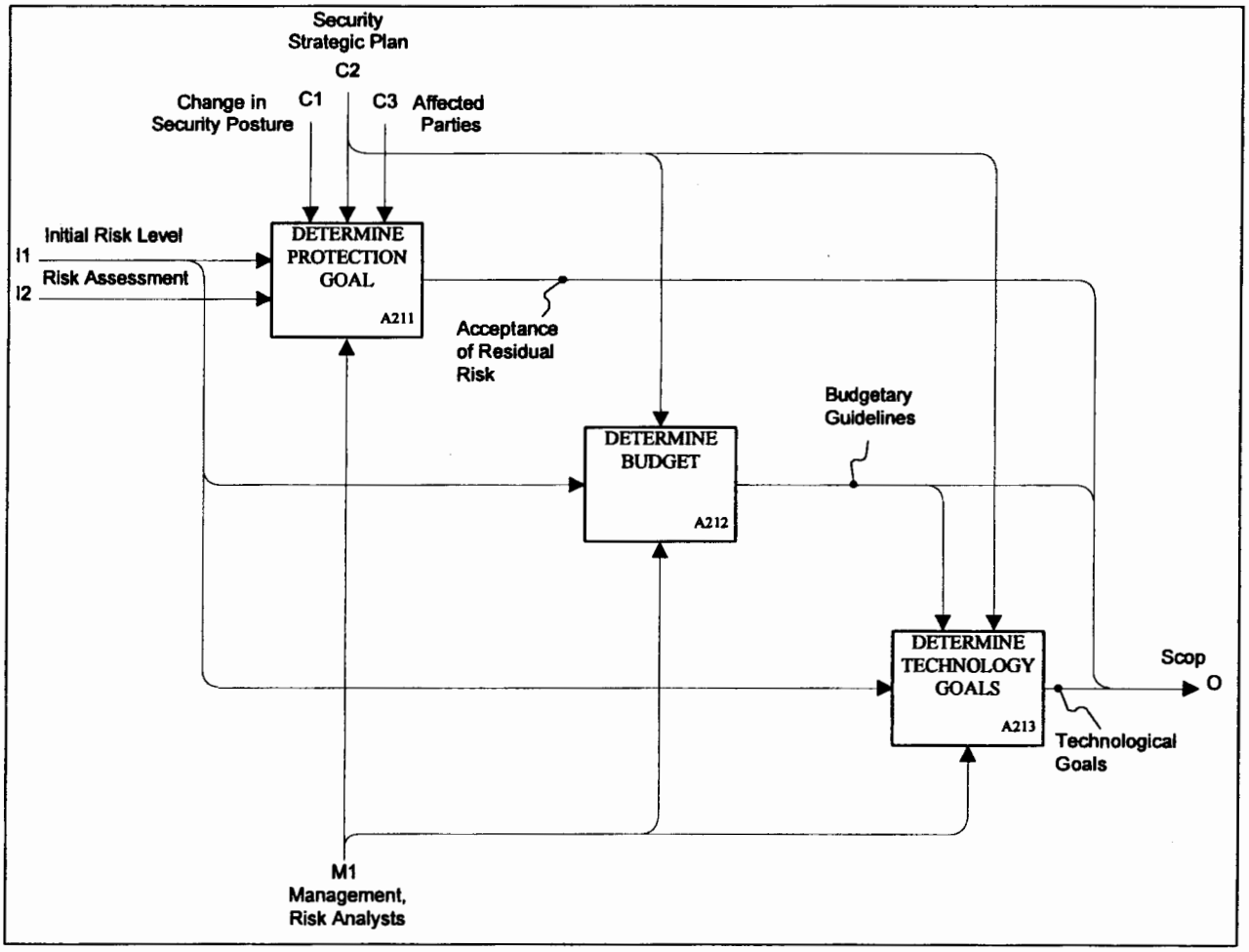


Figure 8. Define Scope

The first step in defining the scope, the identification of the specific protection level goals (Determine Protection Goal, A211), is essential. Risk can never be completely eliminated. Furthermore, the cost of protection can be extremely high and the expectations of the various groups involved may conflict. The tactical security objectives are derived in part from the overall Security Strategic Plan to ensure that risk management of the security system under evaluation conforms to the overall organizational goals. Protection level goals also take into

account the identification of the constraints and compromises (e.g., affected parties, changes in security posture) in order to achieve the optimum level of protection with the most efficient use of resources. The tactical security objectives should state, in as quantifiable terms as possible, the level of protection desired. This may be in terms of minimum loss objectives or in reductions of threat likelihood.

A fundamental constraint on risk management is the amount of funds available to spend on protection. Typically, security or risk management budgets are determined on an annual basis (Determine Budget, A212). It may be impossible to implement all of the desired countermeasures with the funding available. The importance of identifying and working within budgetary constraints becomes evident later in the process when security planners must Determine and Prioritize Critical Assets (A31114, refer to Section 4.3.1.1, Figure 14) and Rank Countermeasures (A43, refer to Section 4.4, Figure 21) in order to made decisions about what countermeasures will best meet protection goals within budget.

The use of new technologies can reduce human error or improve accuracy and effectiveness. Sometimes the technology may have been only partially tested or have lifecycle costs which outweigh its advantages. The use of technology must be specified in explicit goals (Determine Technology Goals, A213) that are defined and accepted by the security team in order to facilitate the countermeasure selection process. Establishing protection goals (Determine Protection Goal, A211), available budget (Determine Budget, A212), and technology goals (Determine Technology Goal, A213) must be established in order to prioritize the type and implementation of countermeasures and determine the level of acceptable residual risk. These difficult decisions and trade-offs should be made at the outset of the project in defining the scope.

4.2.2 Define Boundary [A22]

The system's ***boundary*** defines the extent of the system in question (Refer to Section 2.1 for a definition of the boundary of a system). A boundary in risk management refers to the concise definition of what will and will not be included in the study. An example of a boundary definition may be to examine only high replacement value and *critical assets* to a system's mission. Alternatively, one could perform a more expansive study of *all* assets including critical and supporting systems, i.e., those not critical to a system's mission. Selection of boundaries may be prioritized and then expanded, if time allows, but should not be changed while the investigation is under way without thorough review and concurrence by all affected parties. Changing the boundaries of a system under review may skew the results of the risk assessment and decrease the effectiveness of risk management activities.

4.2.3 Determine Analysis Approach and Tools [A23]

The steps for determining the analysis approach and the corresponding tools to be used in the risk or vulnerability analysis include selecting and identifying the risk analysis methodology (A231) and identifying the tools (A232) and procedures (A233) to be used. The IDEF0 diagram of these steps is shown in Figure 9.

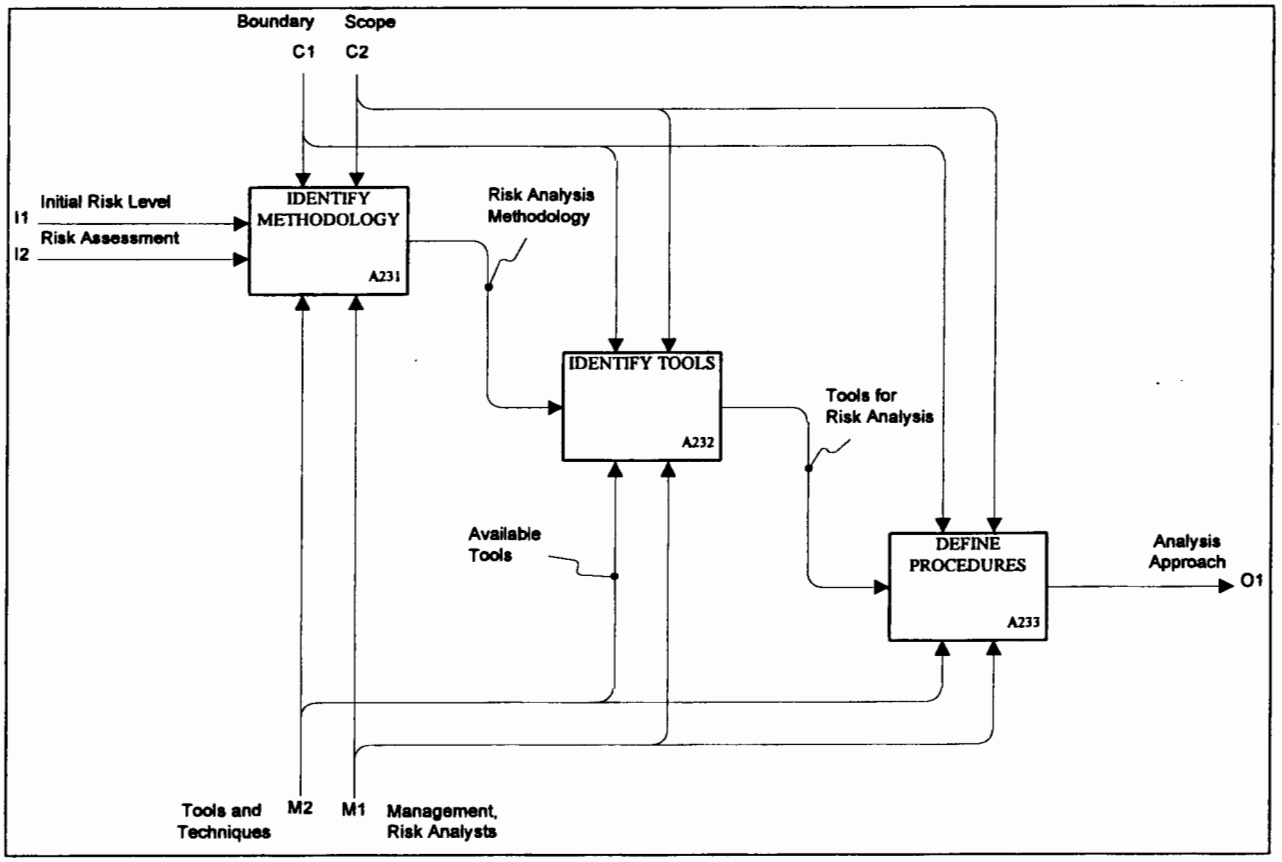


Figure 9. Determine Analysis Approach and Tools

Based on the scope and boundaries of the problem, certain vulnerability and risk assessment methodologies may or may not apply. An initial selection of methods should be made, when options are available, on how the individual process steps will be carried out. This will ensure that the proper data is collected in order to use these methods correctly.

4.2.4 Plan Project [A24]

As in any strategic or tactical planning process, the selection of team members is very important. Team members must represent a good cross-section of the stakeholders if the results of the risk management process are to be broadly accepted. In addition, members should be selected for their analytical skills as well as knowledge of airport security issues.

A schedule should be established and concurrence should be obtained from the working members of the team as well as management. The schedule must detail the specific deliverables and project milestones to be completed during each major project step. The decomposition of the Plan Project activity (A24) is shown in Figure 10.

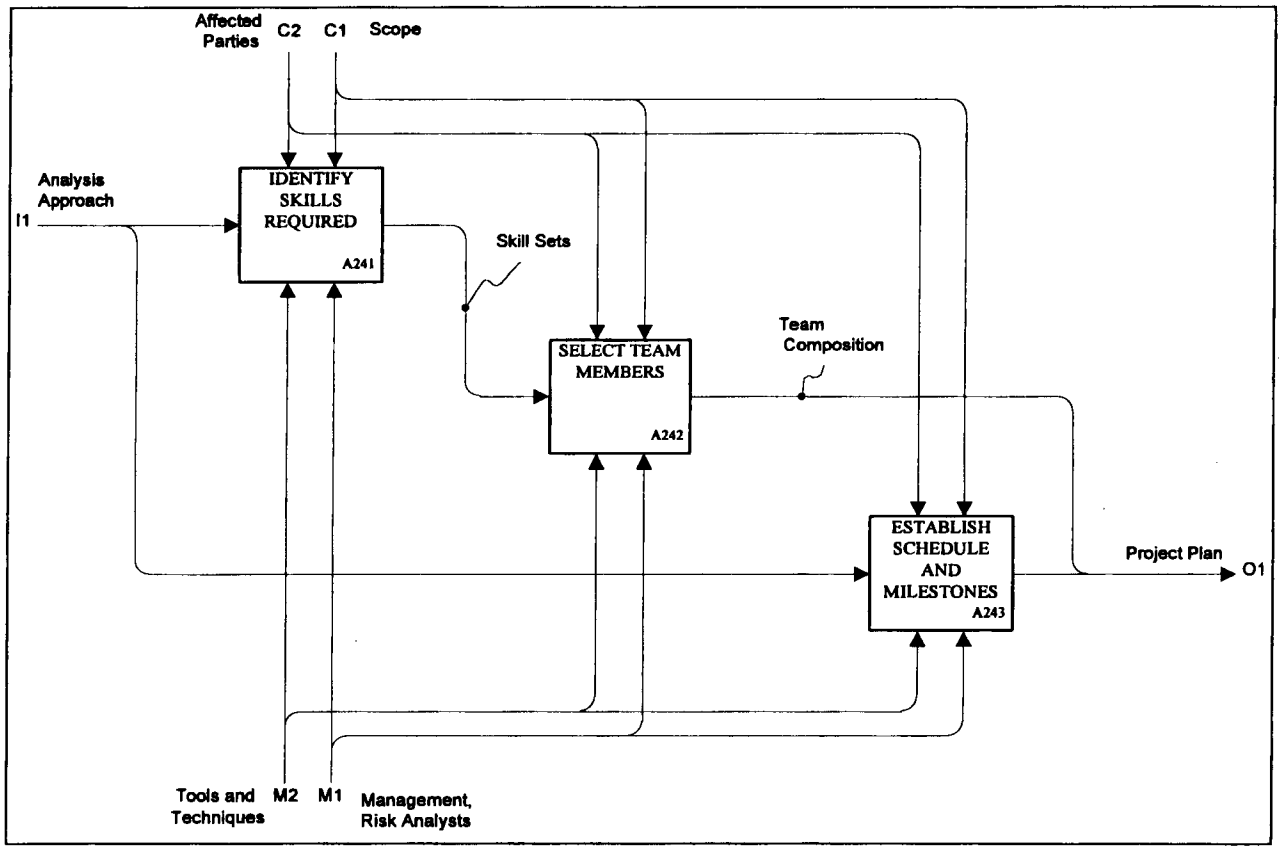


Figure 10. Plan Project

4.3 Assess Risk [A3]

The process of assessing risk is the heart of the Risk Management Process, and also the most complex and intricate step in the process. A risk assessment embodies evaluating vulnerability, determining the likelihood of the system being compromised through a specific vulnerability, and estimating the impact of a vulnerability being exploited by a specific threat. A risk assessment can examine the vulnerability and risk of a system against one threat or include multiple threats, as defined in the scope of the project (activity A21). The process steps for Assess Risk are:

a. Collect Data (A31)
b. Evaluate Vulnerability (A32), and
c. Evaluate Risk (A33).

The IDEF0 diagram of the Assess Risk activity (A3) and the inputs, outputs, controls, and resources of each of the process steps are shown in Figure 11.

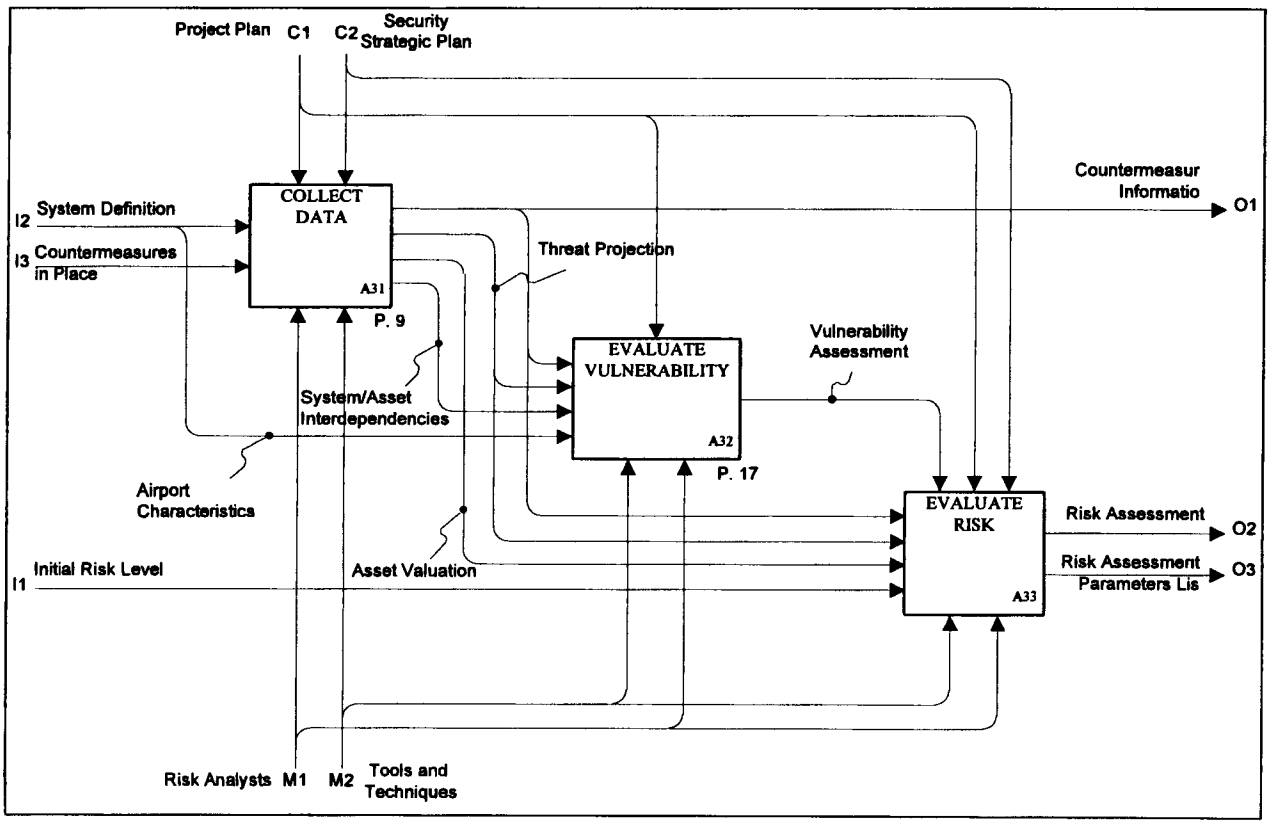


Figure 11. Assess Risk

4.3.1 Collect Data [A31]

Central to all vulnerability assessments is the gathering of data that can be used to uncover vulnerabilities and to form the basis of scientific analysis of alternative countermeasures. The less data or the less accurate the data collected, the greater the uncertainty of the risk assessment results.

The data required to conduct a risk assessment includes asset, threat, and countermeasure data, as shown in the process steps in Figure 12. The Collect Asset Information (A311), Collect Threat Information (A312), and Collect Countermeasure Information (A313) process steps are discussed in Sections 4.3.1.1, 4.3.1.2, and 4.3.1.3, respectively.

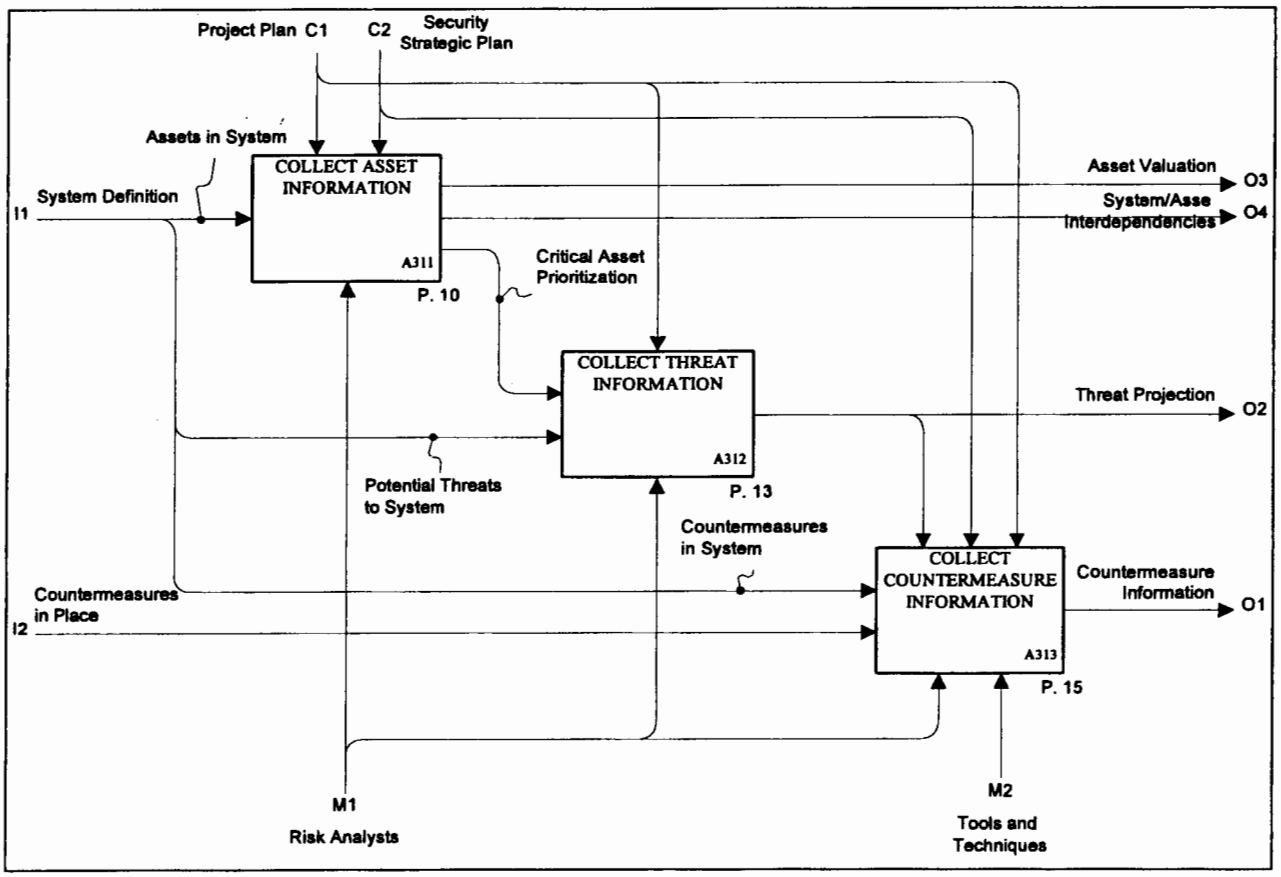


Figure 12. Collect Data

4.3.1.1 Collect Asset Information [A311]

All risk assessment processes focus on the assets to be protected. Assets can be physical installations (buildings, structures, etc.), infrastructures (electrical, fire control, etc.) and other supporting systems (computers, access and control, human organizations, etc.). The value of assets and the role they play in the operation of an airport is therefore very critical to the risk management process. The tactical objectives and the problem definition process steps guide the identification of which assets, infrastructure, and supporting systems will be considered within the boundaries and scope of the risk assessment.

The IDEF0 diagram of the Collect Asset Information activity (A311), shown in Figure 13, consists of three principal steps:

a. Determine and Prioritize Critical Assets (A3111)
b. Establish Dependencies (A3112), and
c. Determine Asset Value (A3113).

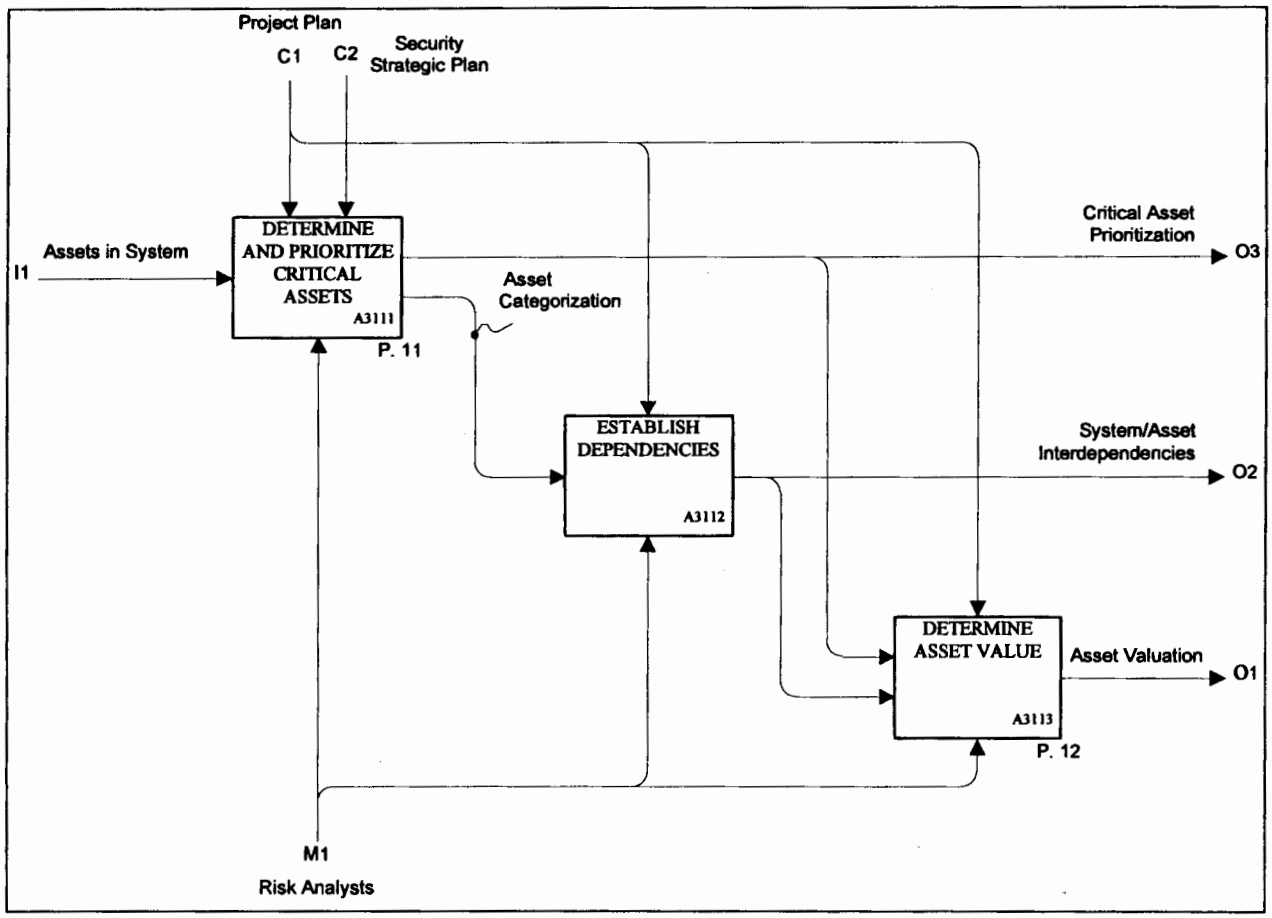


Figure 13. Collect Asset Information

The fist step in collecting asset information is to Determine and Prioritize Critical Assets (A3111), which is decomposed in Figure 14. The identified assets may have characterizations particular to the type of asset and its role in a larger system of components. All of these relationships and qualifiers should be identified. Using the above characterization and categorization process, an attempt is made to determine the assets that are critical to airport operations or have high public visibility (and therefore political impact). The resulting list of critical assets can further serve to limit the scope of the risk management process, without unduly affecting the outcome. This list may be prioritized (by characteristic and category) so that high-impact (critical) assets can be studied first.

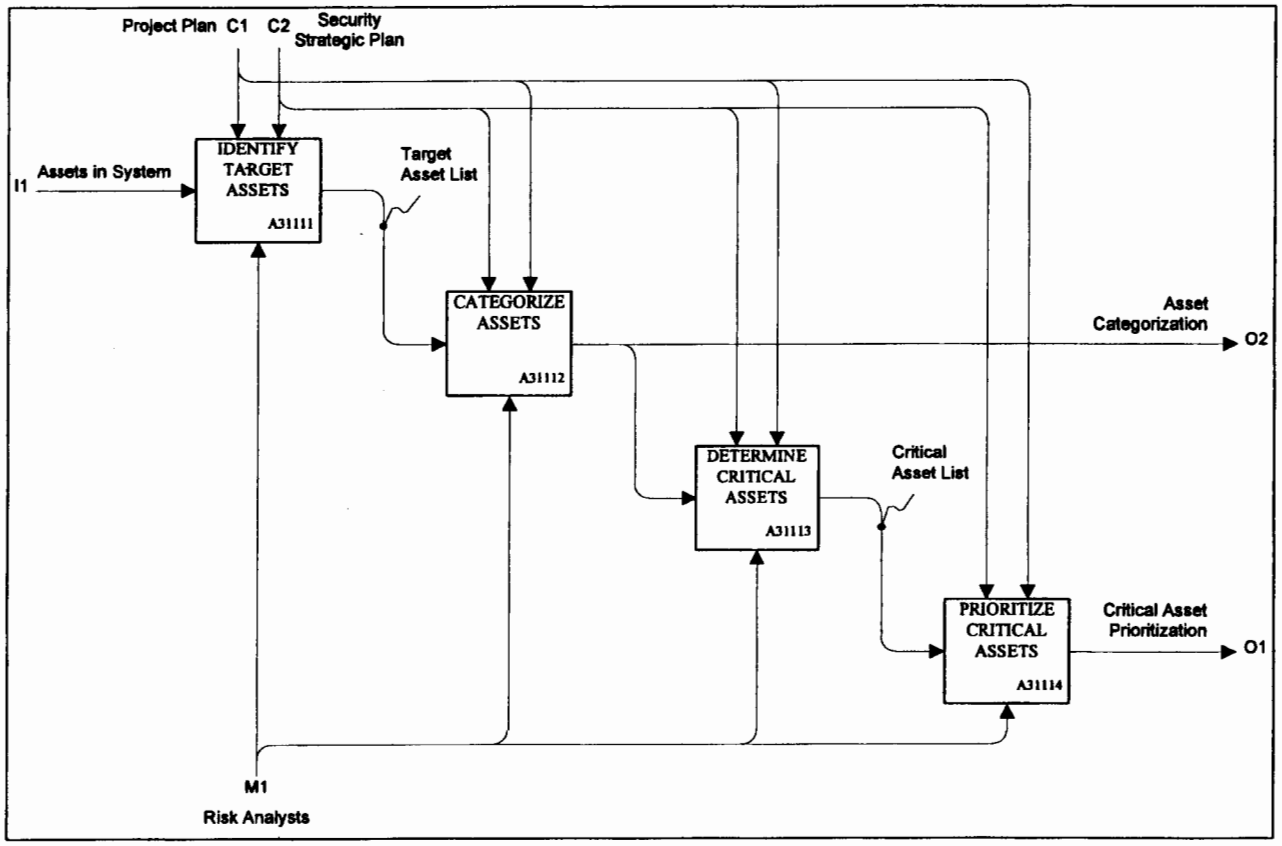


Figure 14. Determine and Prioritize Critical Assets

After critical assets have been identified, the next step is to Establish Dependencies (A3112) between assets within the overall system, i.e., to establish which assets from the asset categorization are contingent upon other identified assets in the performance of the system's mission. (This step has no further IDEF0 decomposition.) The establishment of dependencies becomes important in assessing the impacts on other assets due to loss or damage of a particular asset. The damage to or failure of dependent assets may result in a chain reaction of failures, for example, the failure of the heating and ventilation systems may cause computer equipment to overheat, resulting in a failure of the computer systems to effectively regulate access control.

The final step in the Collect Asset Information activity (A311) is to Determine Asset Value (A3113), shown in Figure 15. Determining asset value is a complex process involving methods for determining costs, including initial value, replacement value, on-going maintenance and lifecycle costs, and indirect costs, such as social or political impacts. It is not cost-effective to protect all assets equally. Critical assets are normally identified as those that have significant impact on operations or are of high value. Critical assets can be facilities, equipment/hardware, personnel, data, or software.

Once the critical assets have been identified and prioritized, their replacement and impact value and the values of their dependent assets should be ascertained. The replacement value includes not only the cost of replacing the asset, but also the cost of installation and operation. Impact values consist of those costs associated with the loss of the asset. They traditionally include the cost of lost asset-related operational capability and impacts on other associated operational capabilities, and the cost to recipients/clients of these lost operational capabilities (e.g., users). The loss of critical assets can result in higher operational costs, lost revenues, passenger delays/inconvenience, and litigation costs. The impact of lost assets can be expressed either quantitatively (e.g., dollars) or qualitatively (e.g., high, medium, or low criticality). The decomposition of the Determine Asset Value (A3113) activity is shown in Figure 15.

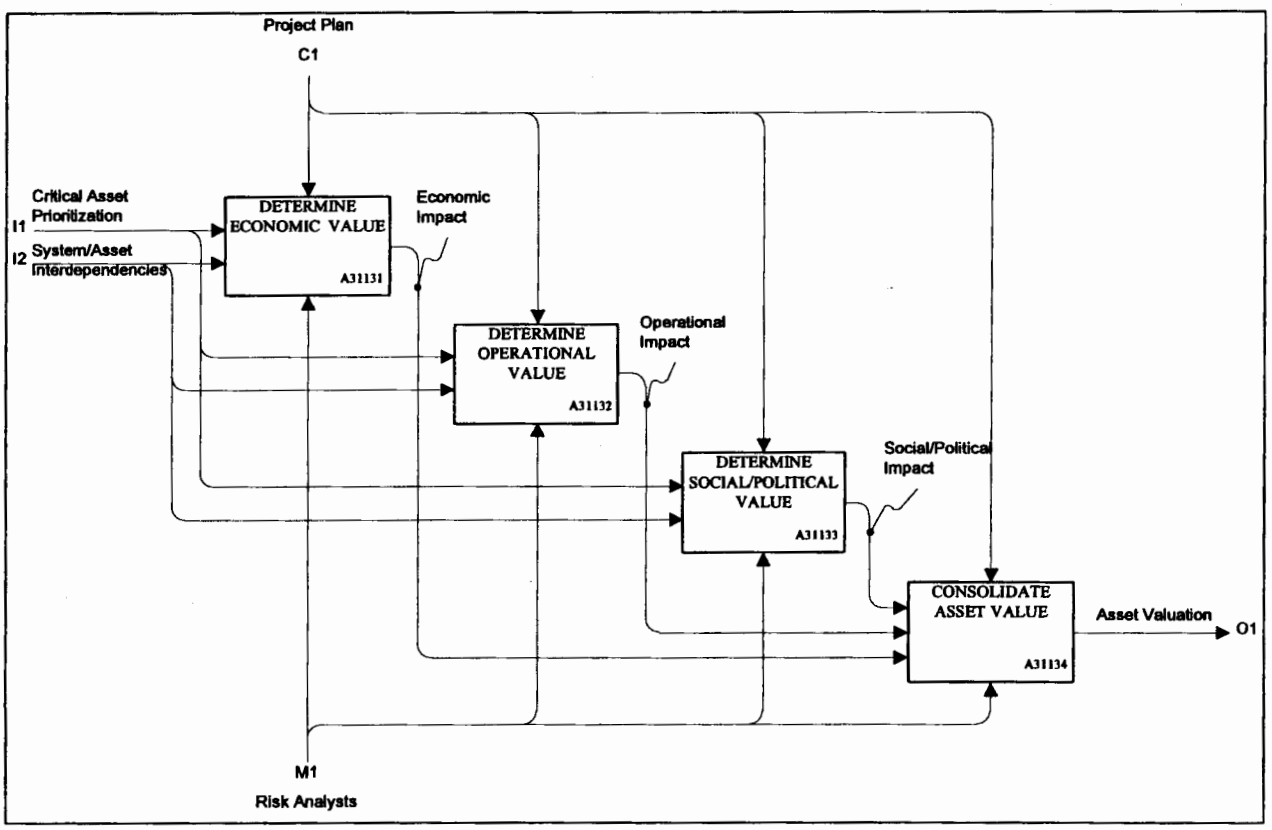


Figure 15. Determine Asset Value

4.3.1.2 Collect Threat Information [A312]

An accurate description of the threat and its likelihood of occurrence is critical to analyzing a threat event. Methods of collecting threat information include profiling the aggressors (Develop Perpetrator Profile, A3121), determining the asset(s) usefulness (Determine Perceived Asset Usefulness, A3122) and availability (Determine Perceived Asset Availability, A3123) to the aggressor, and determining threat likelihood (Determine Threat Likelihood, A3124). Using methods such as research of historical records, both local and national, is necessary to determine likelihood. For threats that have a low frequency of occurrence but potentially catastrophic impact, the use of international threat intelligence and other information from threat projection analyses should be employed. The decomposition of the Collect Threat Information activity (A312) is shown in Figure 16.

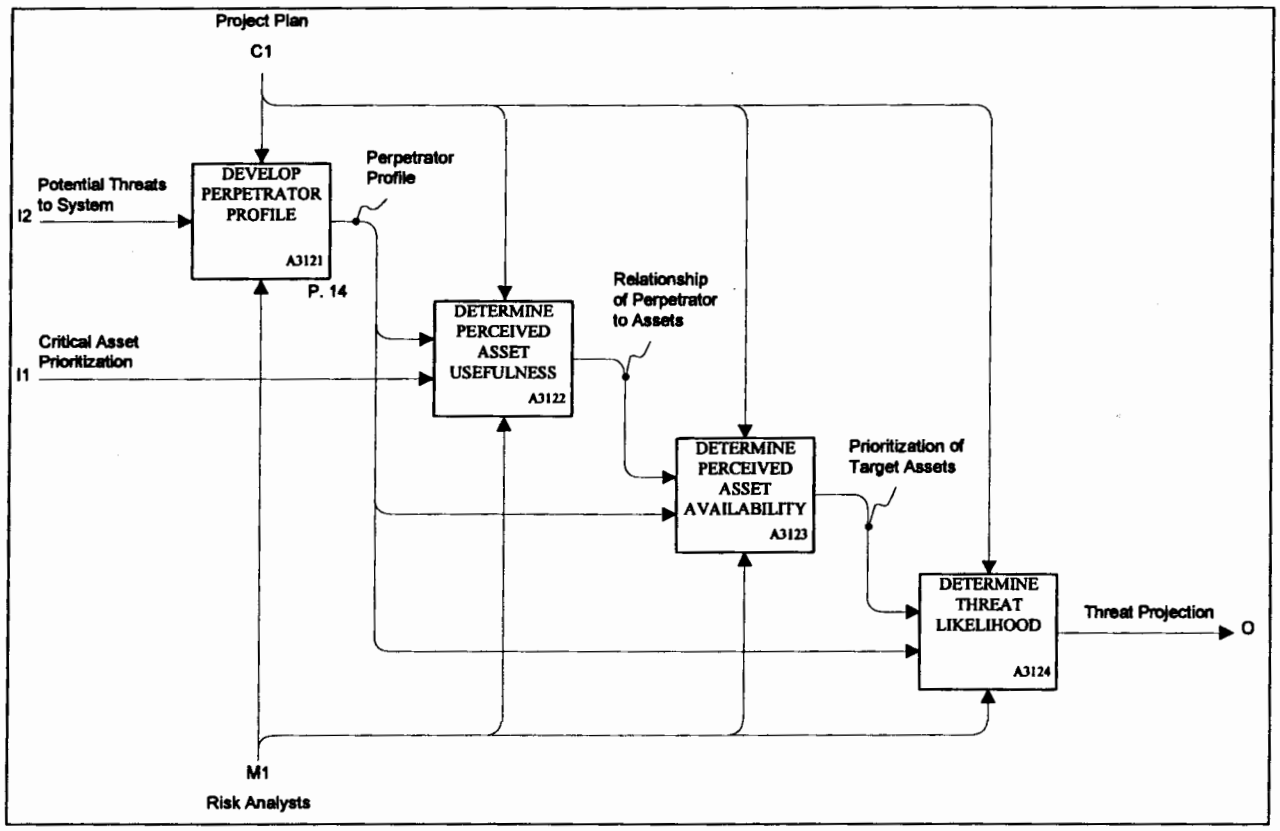


Figure 16. Collect Threat Information

Develop Perpetrator Profile (A3121) breaks down into three steps: Assess General Event History (A31211), Assess Local Event History (A31212), and Collect Intelligence Information (A31213), as shown in Figure 17. General event history refers to the global occurrence of incidents similar to the type of threat being evaluated. For example, the general event history for bombing incidents may include a review of the World Trade Center bombing, the bombing of the Alfred T. Murrah building in Oklahoma City, and the bombing of Pan Am Flight 103 over Lockerbie, Scotland. General event history, as well as all threat data collected, should include criminal or terrorist attempts, threats, and related incidents in addition to successful threat events. The local event history refers to incidents or near incidents occurring in and around the area where the system being evaluated is located, for example, the bomb threats received in the city in question. Intelligence information is often difficult to obtain because of the critical nature of the information. However, to the extent possible, intelligence information should be conducted on both a global and a local level.

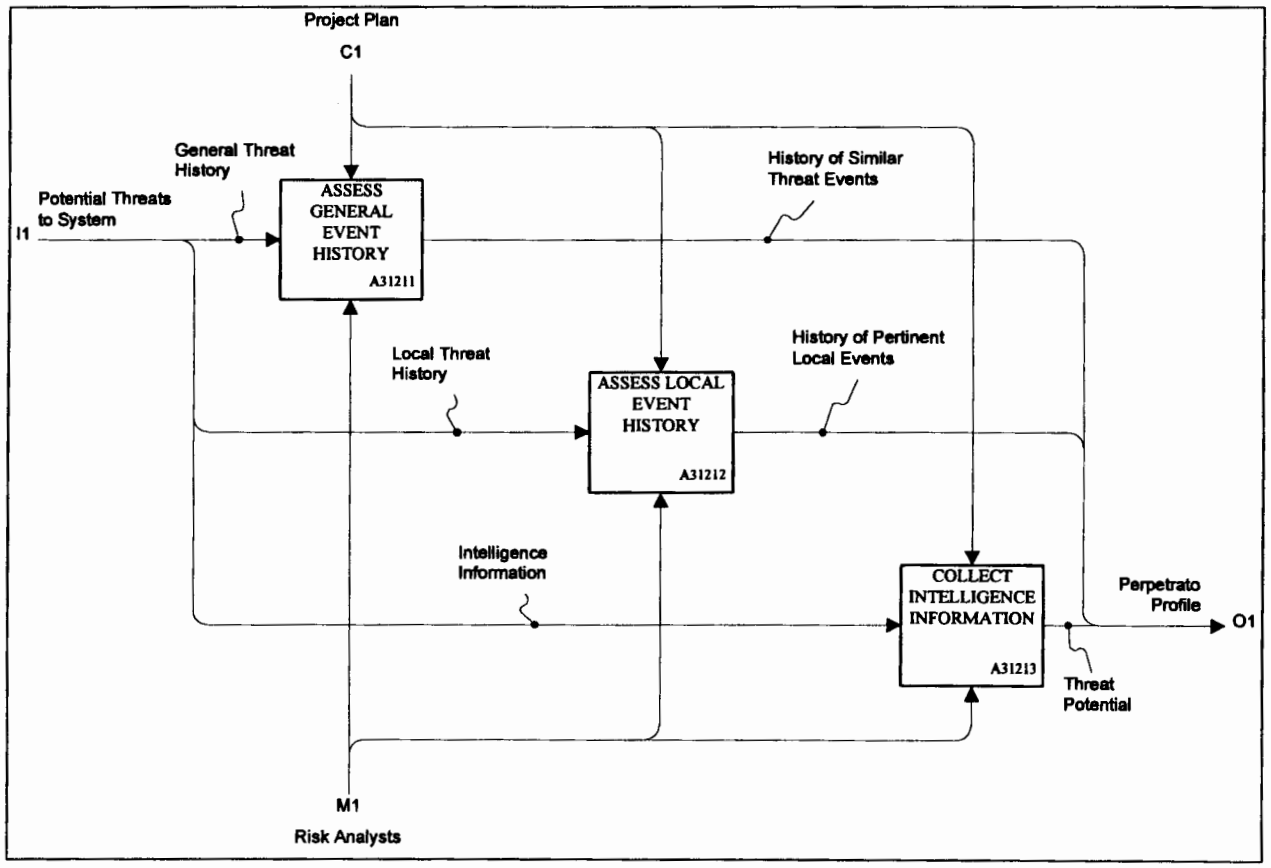


Figure 17. Develop Perpetrator Profile

4.3.1.3 Collect Countermeasure Information [A313]

Countermeasures involve a combination of technological and human factors considerations. In conducting a risk or vulnerability assessment, the existing countermeasures must first be defined in detail to include their intended operational performance and any additional benefits or shortcomings. These countermeasure characteristics must be qualified for each perceived threat. The countermeasures must then be evaluated against established, objective criteria such as costs (e.g., purchase, usage, lifecycle) or pass/fail rates. The three activities under the Collect Countermeasure Information (A313) process step are:

a. Identify Applicable Countermeasures (A3131)
b. Characterize Countermeasures (A3132), and
c. Gauge Countermeasure Effectiveness (A3133).

The Collect Countermeasure Information (A313) decomposition is shown in Figure 18.

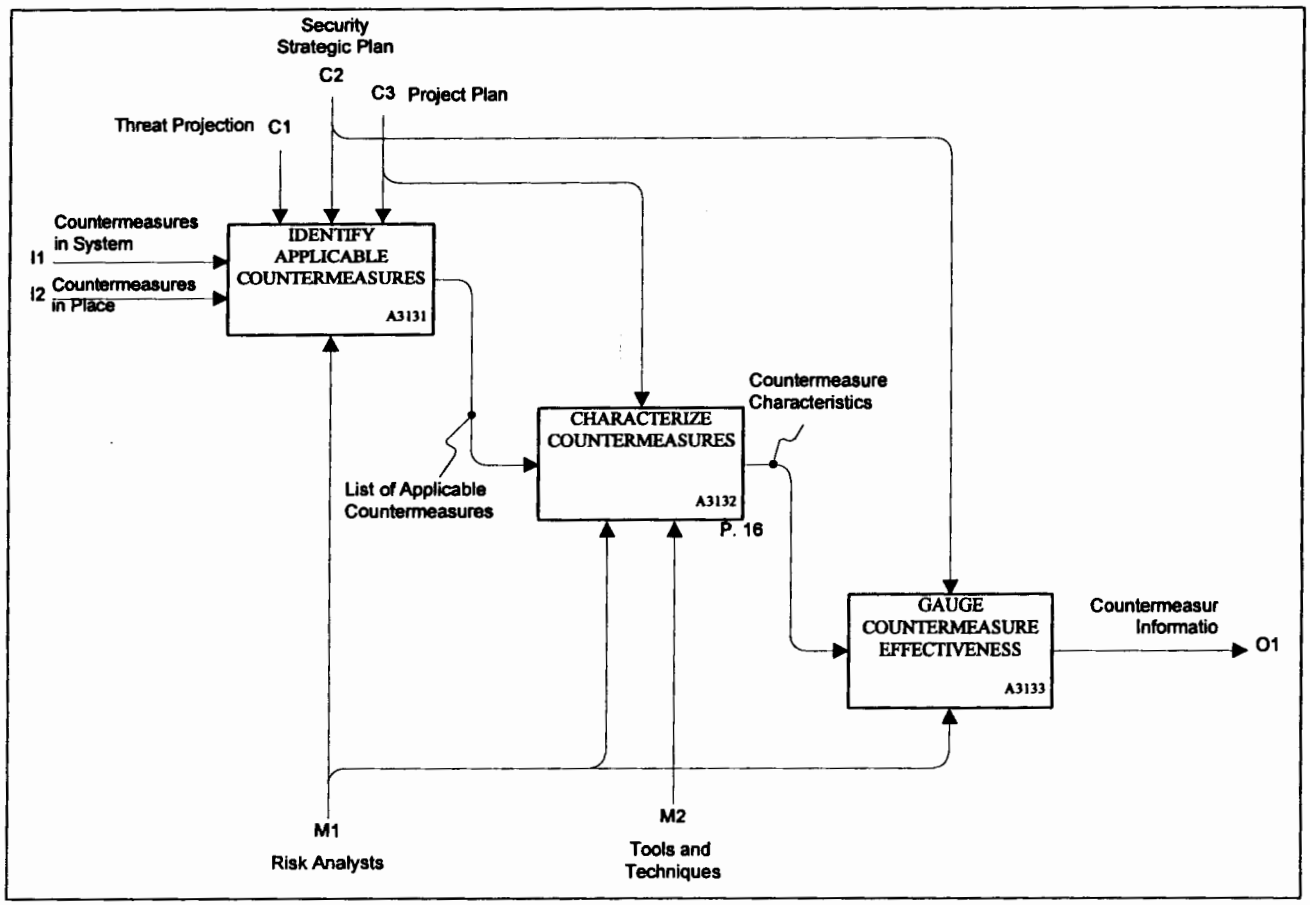


Figure 18. Collect Countermeasure Information

Of the three steps under Collect Countermeasure Information (A313), only Characterize Countermeasures (A3132) is further decomposed, as shown in Figure 19. In defining countermeasure performance, some essential effectiveness parameters should be derived which can be used to quantify the relative merits of alternative countermeasures for trade-off analysis of both existing and proposed countermeasures. The effectiveness of the technology and the operator should be considered as one countermeasure system. Countermeasure system functions can be grouped into the following categories: detection, deterrence, delay, analysis, and response. An example of a detection system is an intrusion detection system. Systems which delay an aggressor include fences, barriers, and housing structures. Analysis capability addresses human factors concerns, such as the ability to expediently recognize an incident displayed on a security monitor. Response capability includes law enforcement, security, and fire and emergency response personnel. Quantitative and/or qualitative methods of assessing capability can be used, and should be defined in process step A23, Determine Analysis Approach and Tools.

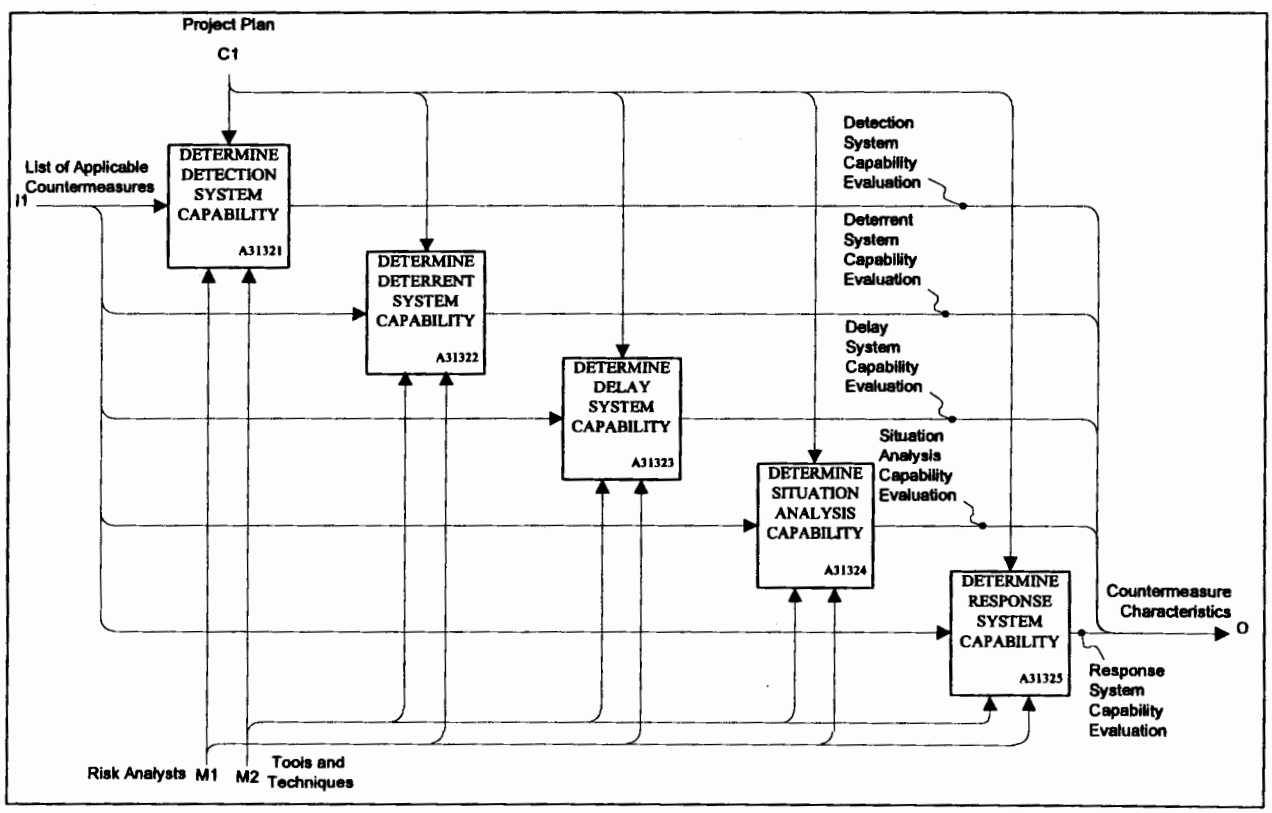


Figure 19. Characterize Countermeasures

Once countermeasures have been identified and characterized, the final step in collecting countermeasure information is to Gauge Countermeasure Effectiveness (A3133) based on the effectiveness parameters identified in the previous step, Characterize Countermeasures (A3132).

The methods and tools used to characterize countermeasures influence the data needs and computational intensity (level of quantification) needed to perform this step in the process. The data needs may be satisfied by simple observations during the operation of a countermeasure or

it may require new and very complex laboratory controlled testing of the various technologies used in the countermeasure system. In all cases, the proper parameterization of the countermeasure is very important, followed by a proper investigation of its effectiveness during operation.

4.3.2 Evaluate Vulnerability [A32]

A comprehensive description of the essential elements of the security environment, i.e., security objectives, assets, threats, and existing countermeasures, provide the baseline used to evaluate vulnerability. Whereas the evaluation of existing countermeasures concentrated on the specific function for which the countermeasure was designed, vulnerability is evaluated for the system as a whole. Vulnerability considers the correlation among all protection systems in the complex environment. Qualitatively, vulnerability is often defined as a lack of an adequate countermeasure. In this case, vulnerable paths are uncovered by security surveys comparing the specific system to a normative ideal. Quantitatively, a vulnerability analysis involves assessing the probability of detecting, assessing, and responding in time to each potential vulnerable path associated with a given vulnerability scenario. The decomposition of Evaluate Vulnerability (A32) is shown in Figure 20.

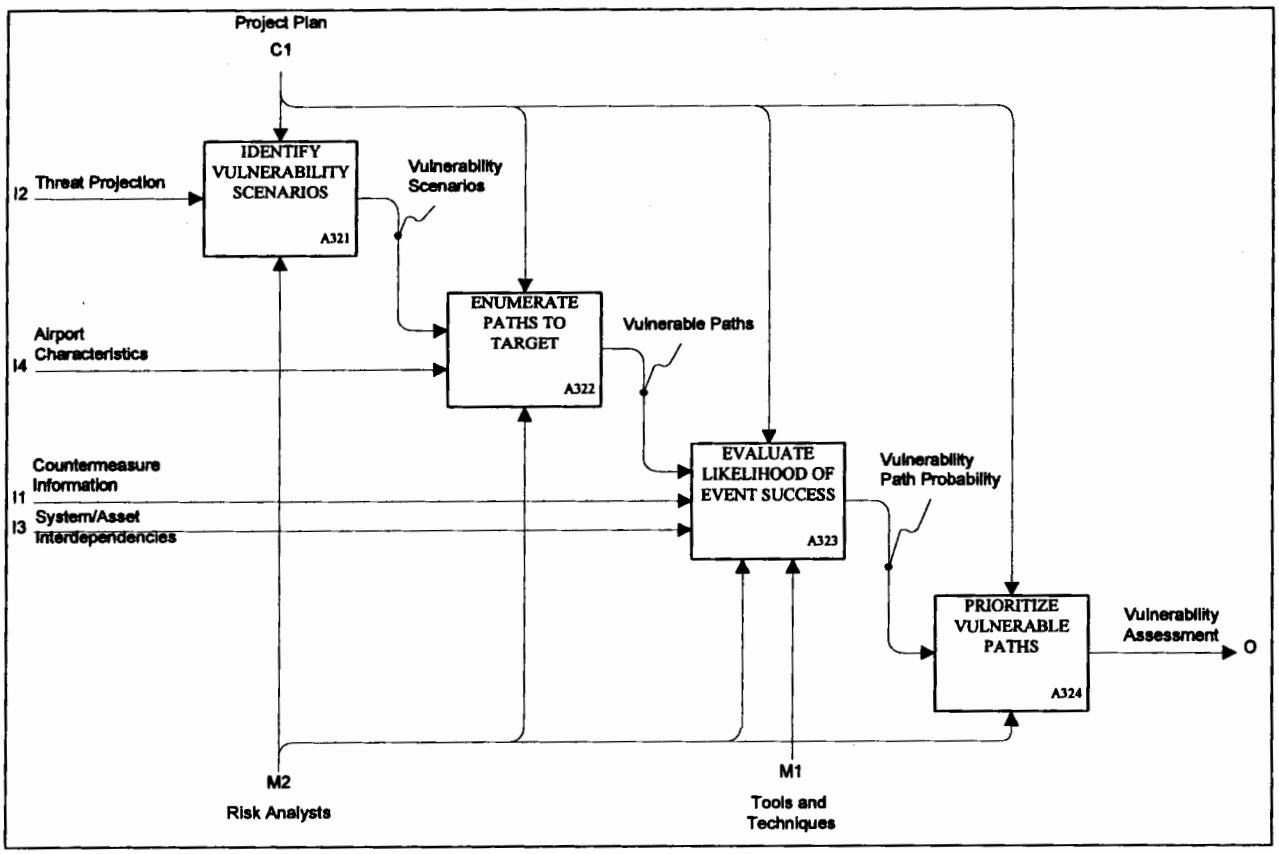


Figure 20. Evaluate Vulnerability

The first step in evaluating vulnerability is to Identify Vulnerability Scenarios (A321). A vulnerability scenario is comprised of an associated perpetrator, threat device, and target. An

example of a vulnerability scenario is the bombing of a federal building in which the perpetrator is a disgruntled employee, the threat device is a simple Improvised Explosive Device (IED) truck bomb, and the target is the Federal building. For each vulnerability scenario, potential vulnerable paths to the target must be identified (Enumerate Paths to Target, A322). Vulnerable paths in the federal building bombing example may include parking a rental vehicle on the street near the building, in an underground garage, or crashing the vehicle into the building. The next step in evaluating vulnerability is to identify the potential success of each vulnerable path (Evaluate Likelihood of Event Success, A323). The likelihood that the perpetrator will achieve his or her goal along a particular path can be considered qualitatively (e.g., rank all paths), or quantitatively (e.g., parametrically determine probability of each path).

A quantitative vulnerability analysis entails a scientific calculation of the probability of intercepting (P_i) the threat. Intercept is defined as successfully detecting, assessing, and setting a response action into motion. Interception may or may not consider the success of the response. For example, the response to an armed aggressor may be initiated, but the success of the resulting firefight is not assured. If it is assumed that the response to an incident will be effective after intercept has occurred, vulnerability (V) in a quantitative analysis equals the likelihood (L_p) that a particular path will be successful for the perpetrator, $V = L_p$. In this situation, L_p is equal to one minus the probability of intercept (P_i), that is, $L_p = (1-P_i)$; therefore $V = (1- P_i)$. That is, the more difficult it is to intercept an aggressor (P_i is low), the more vulnerable the path (V is high).

4.3.3 Evaluate Risk [A33]

Risk is an expression of the probability and impact of an undesired event in terms of event severity and event likelihood. A risk assessment combines the information gained from the Collect Data (A31) and Evaluate Vulnerability (A32) process steps to develop a valuation of impact and likelihood of an undesired event. Whereas vulnerability considered the likelihood of success of a particular *vulnerable path*, a calculation of risk also considers the likelihood of a *threat event* or *threat scenario*. A vulnerability analysis ignores the threat of occurrence of an undesirable event and assumes that the threat is real, i.e., the probability of occurrence is one or 100 percent. Assuming the threat as a given minimizes the uncertainty of predicting the likelihood of a future event, as is required to evaluate risk.

In a risk assessment, the likelihood that a particular threat scenario will be perpetrated against a particular asset within a given timeframe is calculated using data collected in steps A312–Collect Threat Information and A32–Evaluate Vulnerability. The threat information provides data to predict whether a threat scenario will occur along a particular path and the vulnerability information provides data to identify susceptible assets, and these are combined to establish likelihood.

The other component of risk is severity or impact. Determining the impact of a threat event relies on data collected in steps A312–Collect Threat Information and A311–Collect Asset Information. An impact analysis must be performed to place a value on the loss of assets to a particular threat event. The identification and prioritization of critical assets, the interdependencies between various assets, and the asset value all factor into the impact of a threat

event. The threat information important to the impact analysis is the threat device used and, correspondingly, the type and degree of damage it can cause.

The impact assessment is performed by computing the replacement and impact costs associated with critical assets that are destroyed or damaged due to a successful threat event. Total valuation of impact may have to include factors for loss of an asset, interruption in service or operations, and even the political and legal consequences of the event. Direct costs of a loss, such as initial and replacement costs, are relatively straightforward. Indirect costs are more difficult to quantify.

Impact is frequently expressed as an economic factor, for example, the representation of risk is expressed as annual loss expectancy (ALE). The ALE is the likelihood-of-loss times the impact of that loss in dollars. As discussed in Section 2.2, Methods of Estimating Risk, ALE is a quantitative risk measurement. Risk may also be expressed relatively, i.e., a ranking of threat scenarios from greatest to least risk or an expression of low/medium/high risk.

4.4 Select and Implement Countermeasures [A4]

Essential to the risk management process is a method for the selection of appropriate and cost effective countermeasures. Since there are a great many countermeasures, each with a unique set of advantages and disadvantages against a given threat, the selection process is multi-dimensional. There is a near infinite set of combinations of existing countermeasures. To that list is a growing number of new, technologically based countermeasures. The output of this process step will provide feedback to management on available alternatives for the selection of new countermeasures and in the on-going process of risk management (constant reevaluation based on new data). The process steps for Select and Implement Countermeasures (A4), presented in Figure 21, are discussed below.

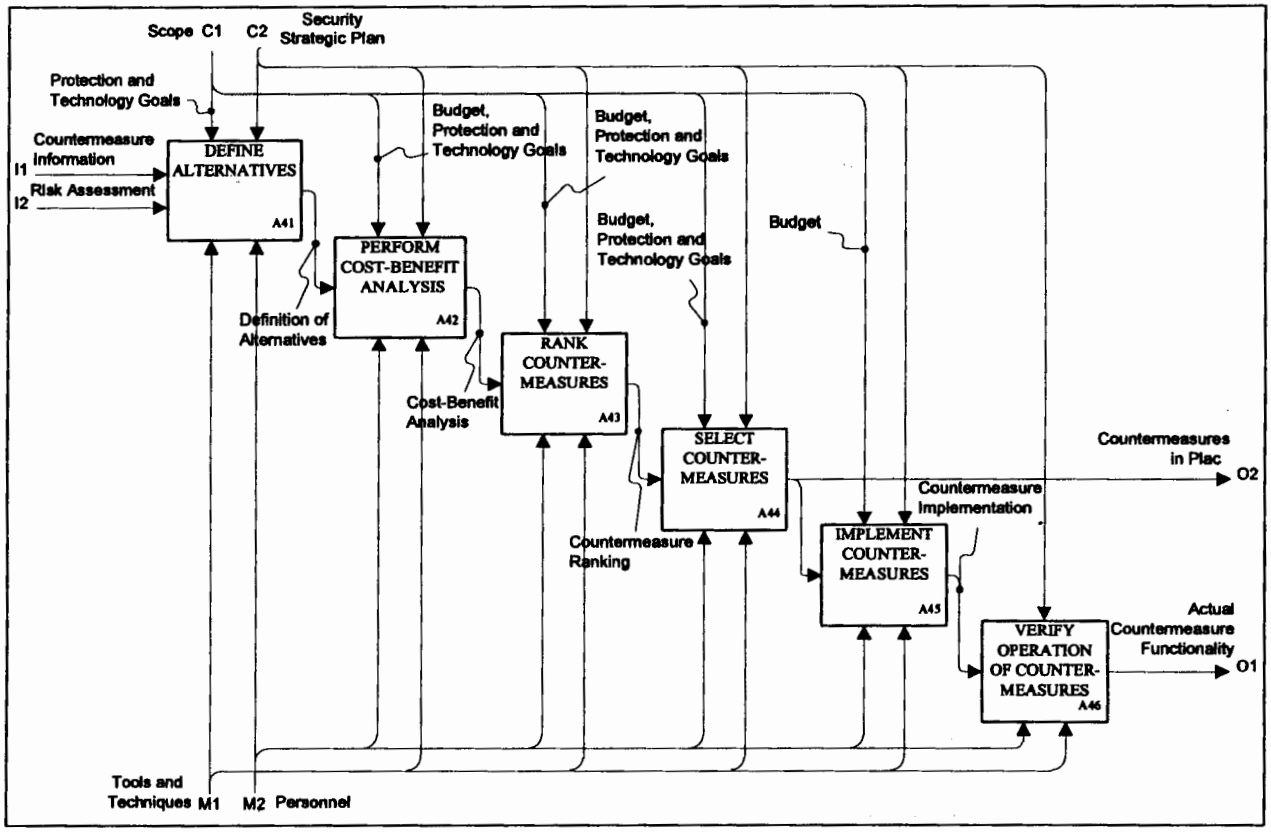


Figure 21. Select and Implement Countermeasures

The first step is to define the available alternatives (A41). Existing and planned countermeasures should both be considered. The Collect Countermeasure Information (A313) step discussed above should provide the data input in a sufficiently quantitative format to allow for ranking of alternatives by various factors such as cost, relative effectiveness against specific threats, and other parameters. The countermeasures selected for review should then be assembled into a system. It is the effectiveness of the entire countermeasure system that is to be evaluated. Most often, the type of evaluation performed is a cost-benefit study (A42).

Cost should include factors for both direct and indirect costs and benefits must be expressed in both quantitative and qualitative terms. The selection of countermeasures to be implemented should be influenced by this cost-benefit study. Also to be considered is the degree of difficulty in implementation and maintenance of the selected systems. Mechanisms for automatically monitoring the performance of the installed systems should be directly integrated into the systems, if possible.

Many methodologies can be used to rank countermeasures (A43). Most rely on both cost and an analysis of effectiveness. The ranking should be broad enough to include operational and technological solutions and consider various configurations of the same components as alternative solutions. The selection of countermeasures (A44) can be made using decision sciences tools, such as weighting factors, selection matrixes that include qualitative as well as quantitative factors, and expert opinion. The implementation of the changes to the countermeasure system (A45) should be controlled so as to facilitate the measurement of

effectiveness and cost before and after implementation. After implementation , a planned period of evaluation (A46) with predefined experiments or operational tests should be performed to ensure that the new system performs as planned.

4.5 Monitor Countermeasure Effectiveness and Changes in Risk Factors [A5]

Feedback is an essential element in the overall risk management process. Effective security management requires constant vigilance. Not only is it important to ensure that the existing and upgraded countermeasure systems are functioning properly, but, the threat situation has to be continually evaluated and the baseline data has to be constantly reviewed (new assets, construction impacts, newly uncovered vulnerabilities). This process step is shown Figure 22.

Planned, periodic reviews of the risk assessment should be institutionalized. Large complex facilities in rapidly changing environments should be re-evaluated annually. Slowly evolving threat situations affecting static facilities could be reviewed as little as once every three years.

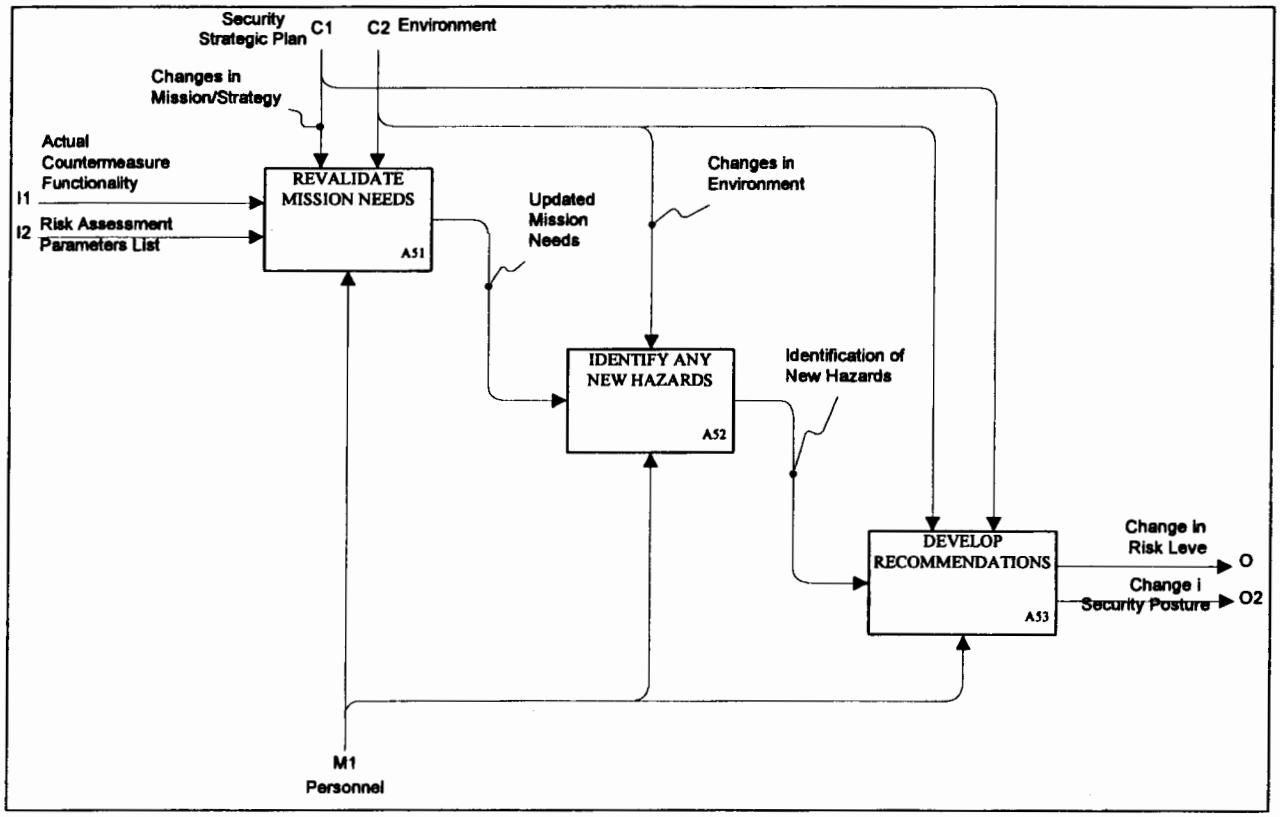


Figure 22. Monitor Countermeasure Effectiveness and Changes in Risk Factors

5. BIBLIOGRAPHY

The following documents are related to the FAATC Risk Management Process R&D project:

a. FAATC Technical Report DOT/FAA/AR-96/1, *Functional Methodology for Risk Management*, December 1996.

b. FAATC Technical Report DOT/FAA/AR-97/1, *Evaluation of the Security Analysis Support System (SASSy) Customized for Civil Aviation Security*, January 1997.

c. FAATC Technical Report, *Assessment of Airport Security Environment*, August 1997.

d. *Airport Vulnerability Assessment Master Plan*, Abacus Technology Corporation, December 1997.

e. *Denver International Airport (DEN) Vulnerability Assessment Report*, Abacus Technology Corporation, September 1998, and

f. *Detroit Metropolitan Wayne County Airport (DTW) Vulnerability Assessment Report*, Abacus Technology Corporation, September 1998.

Additional risk management and project references:

a. Federal Information Processing Standards Publication 183, *Integration Definition for Function Modeling (IDEF0)*, National Institute of Standards and Technology, December 21, 1993.

b. *Final and Strategy Report*, Commission of European Communities Security Investigations Projects, Project S2014 - Risk Analysis, Version 1.0, February 1993.

c. Federal Information Processing Standards Publication 191, *Guideline for the Analysis of Local Area Network Security*, National Institute of Standards and Technology, November 9, 1994.

d. *Framework for Environmental Health Risk Management*, Final Report, Volume 1, The Presidential/Congressional Commission on Risk Assessment and Risk Management, 1997.

e. *Quality Assurance Review Guide for Major Information Resources Projects*, Version 1.0, Quality Assurance Team, Department of Information Resources, Office of the State Auditor, Austin Texas, November 1996.

f. Guttman, Barbara and Edward Roback, National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

g. Department of the Army Pamphlet 190-51, *Risk Analysis for Army Property*, September 30, 1993.

h. Snell, Mark, *GSA Risk Assessment Matrix (RAM) Evaluation*, Sandia National Laboratories, February 1992.

i. *Understanding Risk: Informed Decisions in a Democratic Society*, National Resource Council, June 1996.

j. *Risk Assessment and Risk Management in Regulatory Decision-Making (Draft Report)*, Environmental Protection Agency, Commission on Risk Assessment and Risk Management, June 13, 1996.

k. FAATC Technical Report DOT/FAA/CT-94/49, *Security Analysis Framework*, Volumes I-III, September 1994.

l. *Computer Security Risk Analysis for the Anchorage, Alaska ARTCC Computer Facility*, FAA Office of Civil Aviation Security, January 15, 1987.

m. *FAA System Safety Handbook (Draft)*, FAA Office of System Safety, October 1996.

n. Caskey, David, *Risk Identification: Threat Evaluation vs Vulnerability Assessment*, Sandia National Laboratories presentation made at the AAAE Airport Security Seminar in Alexandria, VA, June 28, 1991.

o. Sui, Nathan, *Probabilistic Risk Assessment: Potential Application in Aviation Security*, Center for Reliability and Risk Assessment of the Idaho National Engineering Laboratory, presentation made at the SPIE 1992 International Symposium on Optical Applied Science and Engineering in San Diego, CA, July 19-20, 1992.

p. Jablonowski, Mark, "Expert Systems for Risk Management," Risk Management, September 1992.

APPENDIX A

FAA WILLIAM J. HUGHES TECHNICAL CENTER RISK MANAGEMENT PROCESS

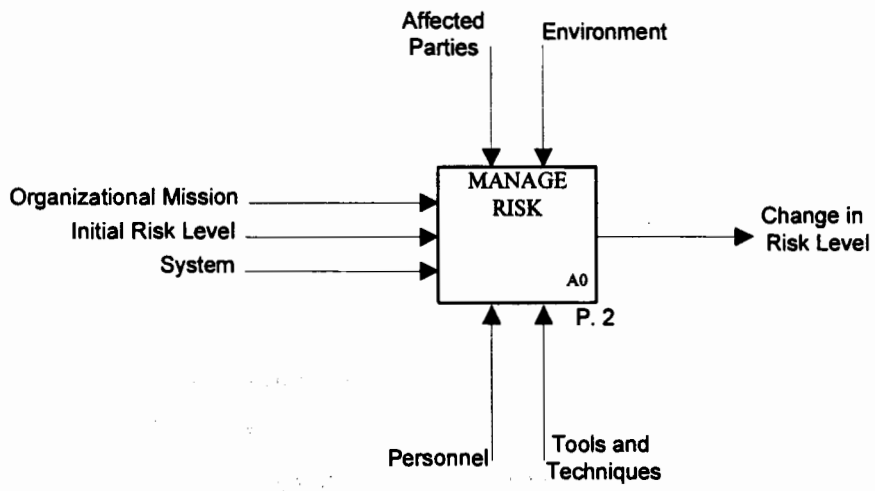
This page intentionally left blank.

Appendix A: FAA William J. Hughes Technical Center Risk Management Process

The following pages contain an IDEF0 representation of the complete process for managing the security risk at the nation's airports (referred to in Section 3 of this document). Abacus Technology has fully defined a process for vulnerability assessments, risk assessments, and risk management of aviation security issues. This process was used to perform airport vulnerability assessments for the Airport Vulnerability and Analysis Project.

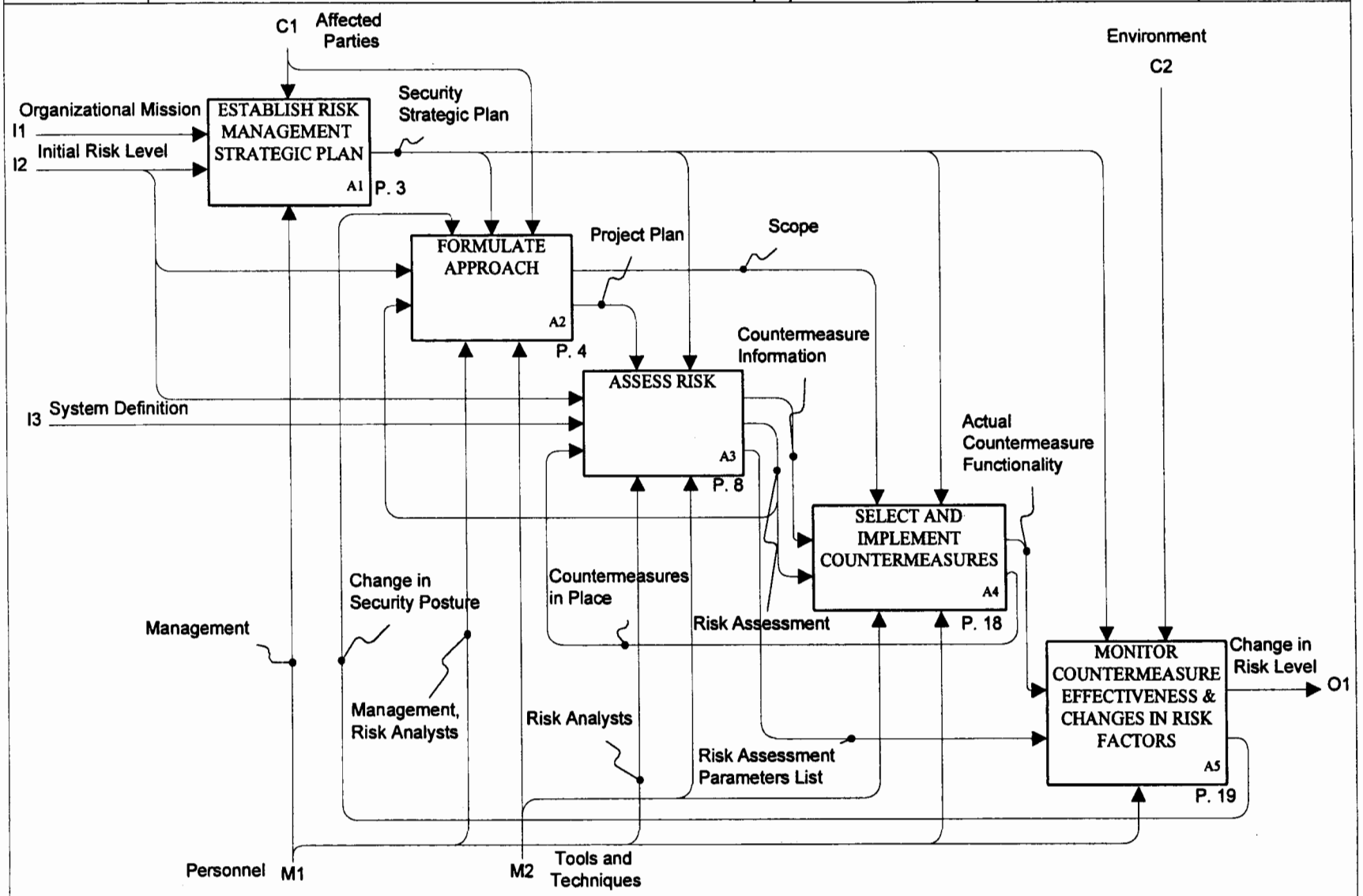
This page intentionally left blank.

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			Top
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



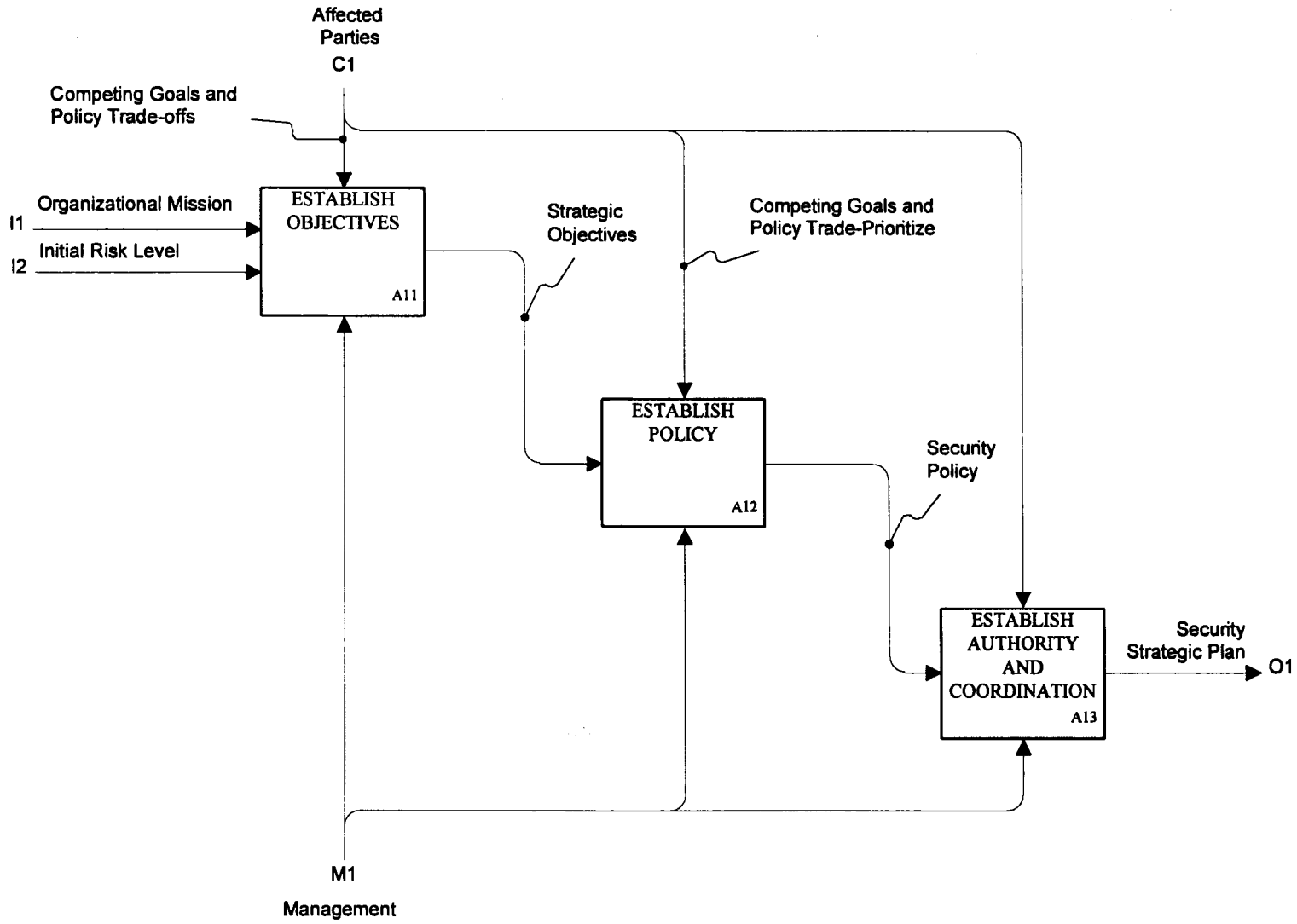
NODE: A-0	TITLE: FAA Technical Center Risk Management Process	NUMBER: P. 1

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 06/22/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
	NOTES: 1 2 3 4 5 6 7 8 9 10			RECOMMENDED			
			x	PUBLICATION			



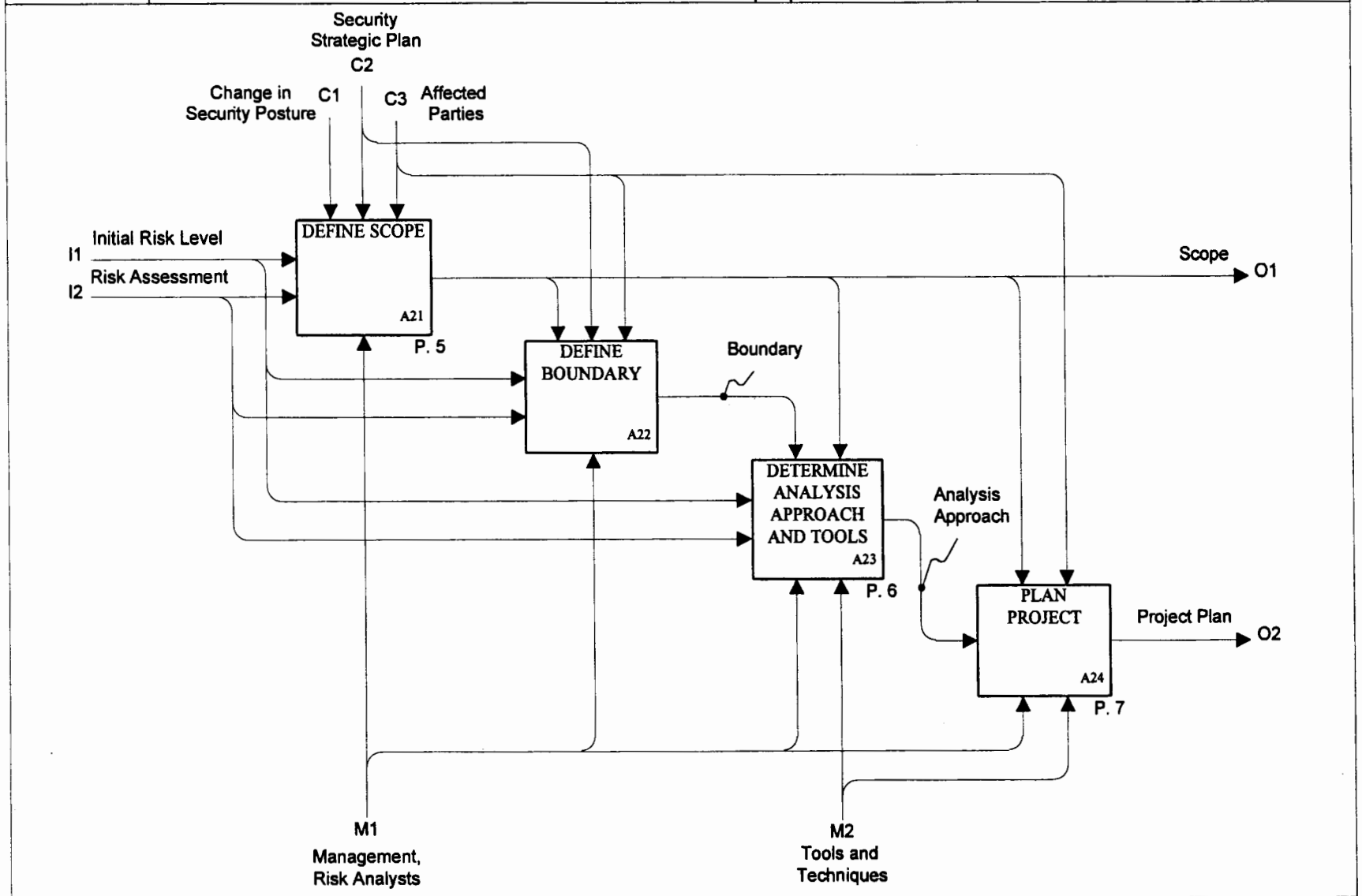
NODE: A0	TITLE: MANAGE RISK	NUMBER: P. 2

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
	NOTES: 1 2 3 4 5 6 7 8 9 10			RECOMMENDED			
			x	PUBLICATION			



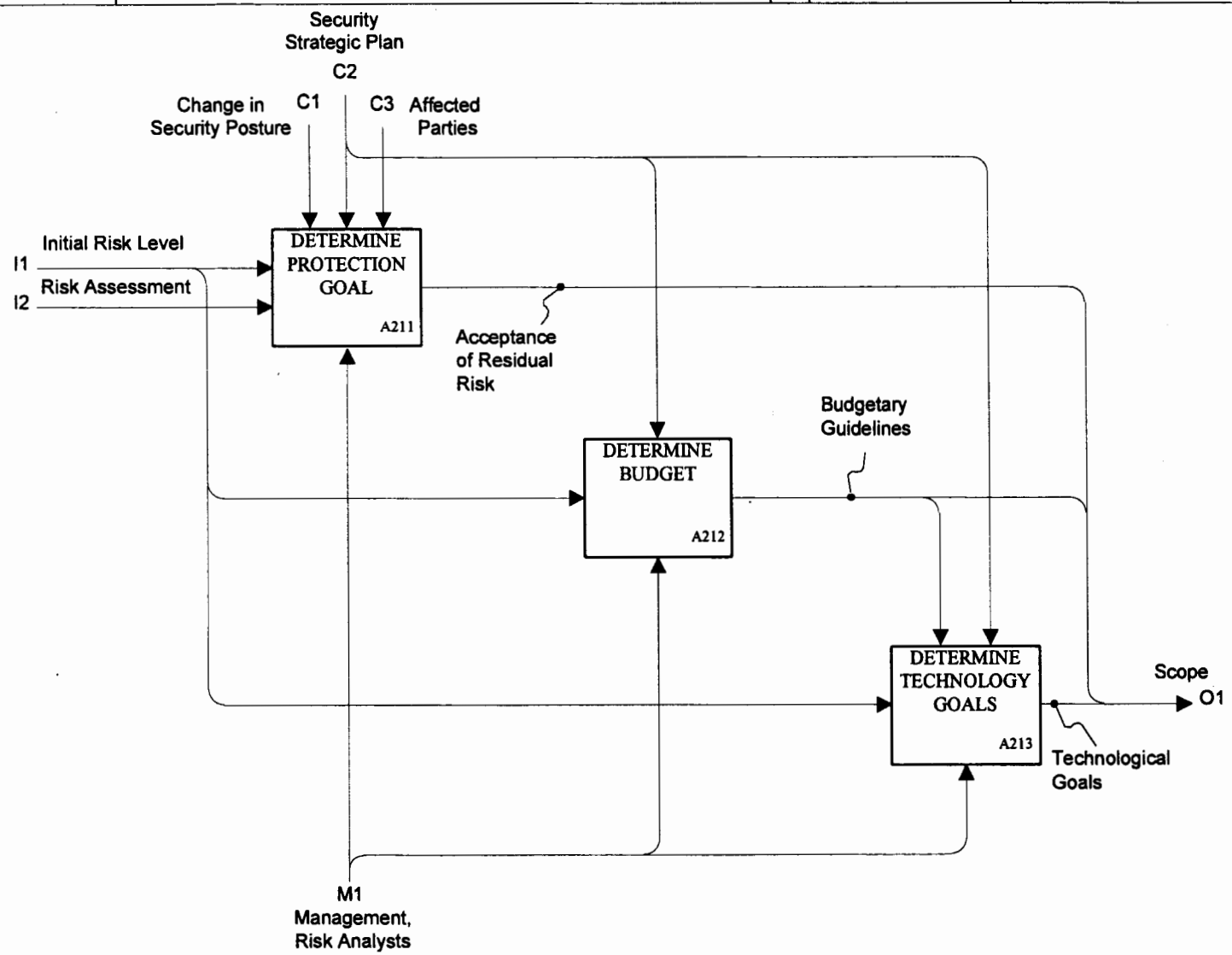
NODE: A1	TITLE: ESTABLISH RISK MANAGEMENT STRATEGIC PLAN	NUMBER: P. 3

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



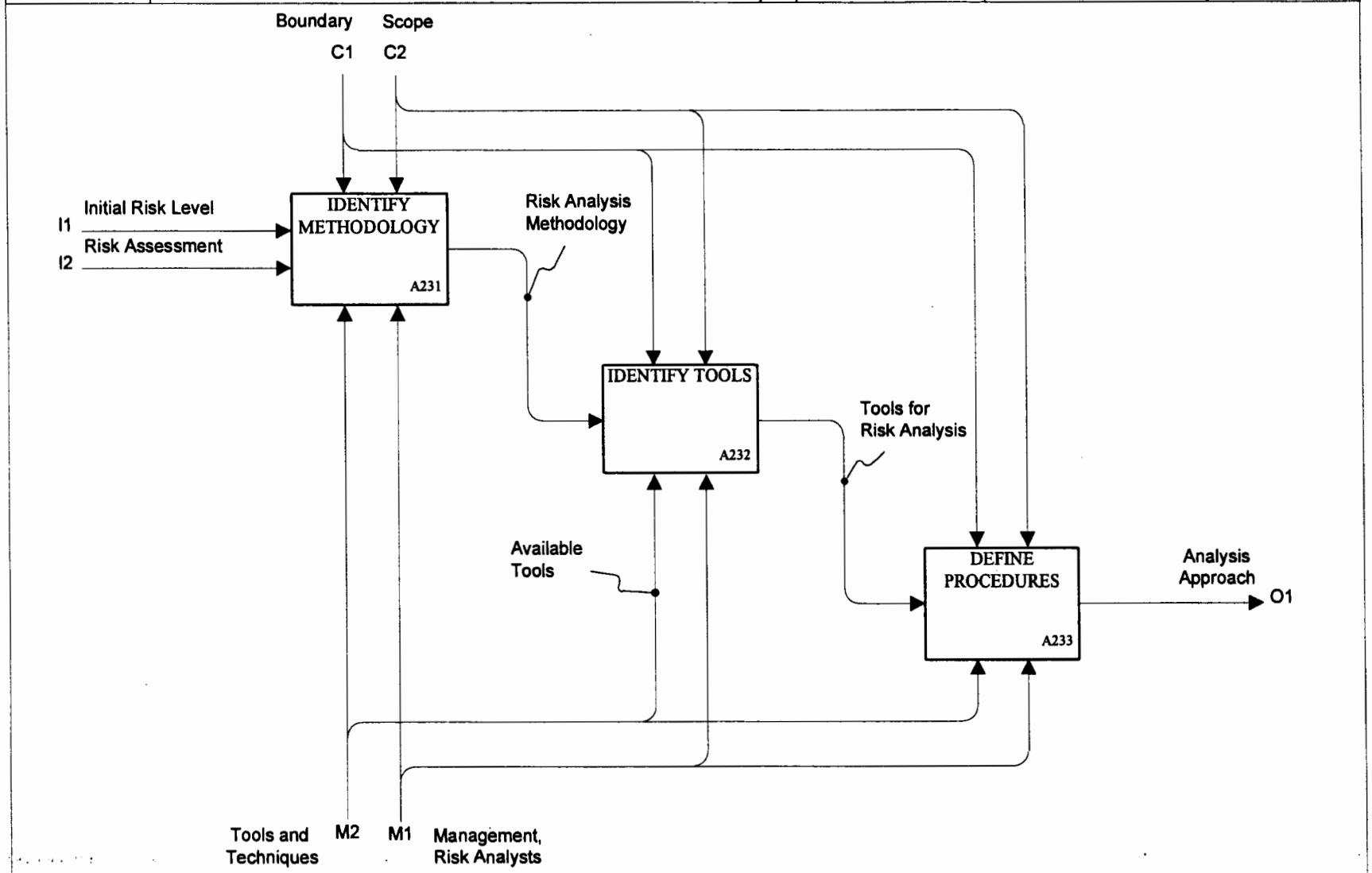
NODE: A2	TITLE: FORMULATE APPROACH	NUMBER: P. 4

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



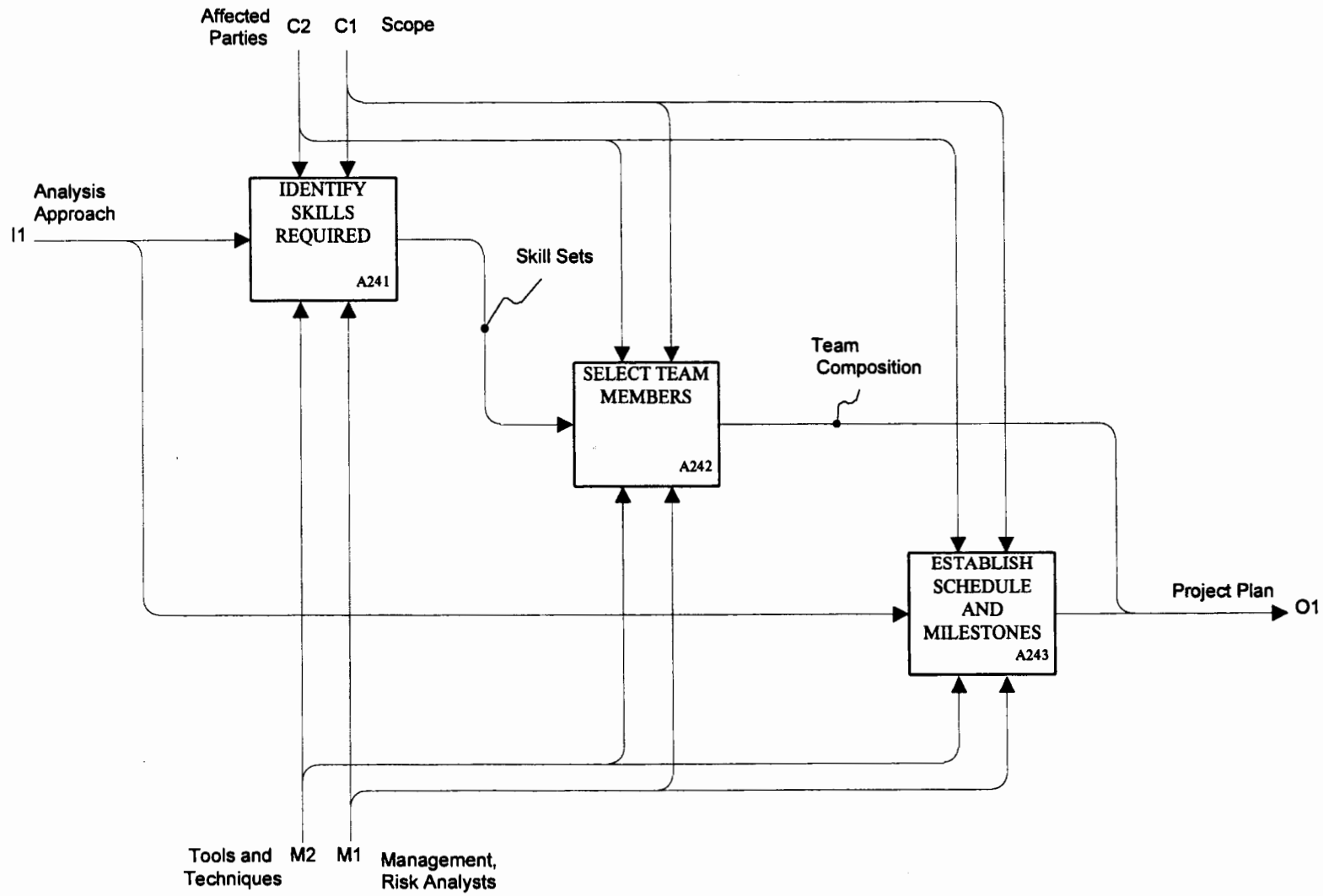
NODE: A21	TITLE: DEFINE SCOPE	NUMBER: P. 5

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



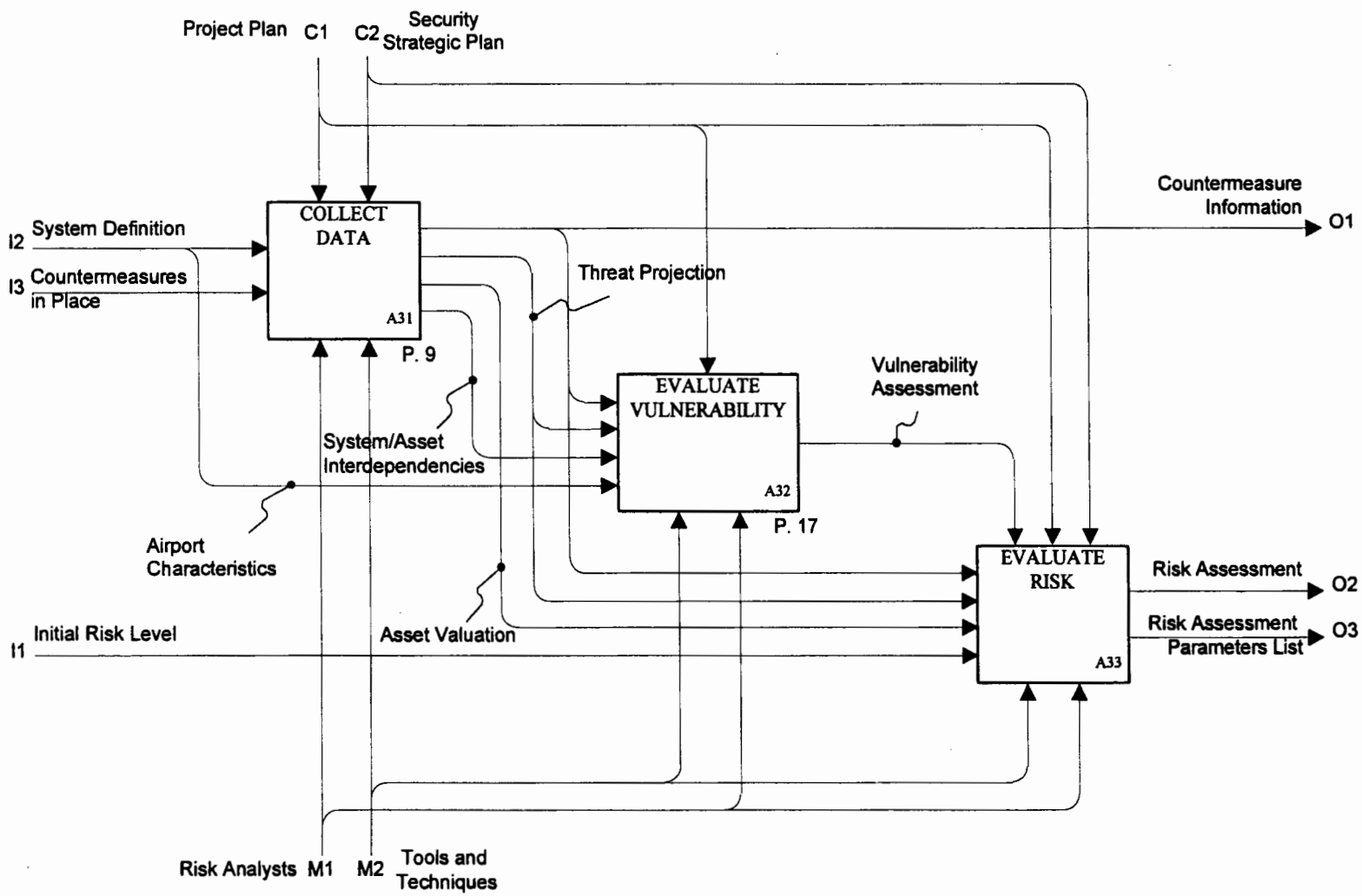
NODE: A23	TITLE: DETERMINE ANALYSIS APPROACH AND TOOLS	NUMBER: P. 6

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
	NOTES: 1 2 3 4 5 6 7 8 9 10			RECOMMENDED			
			x	PUBLICATION			



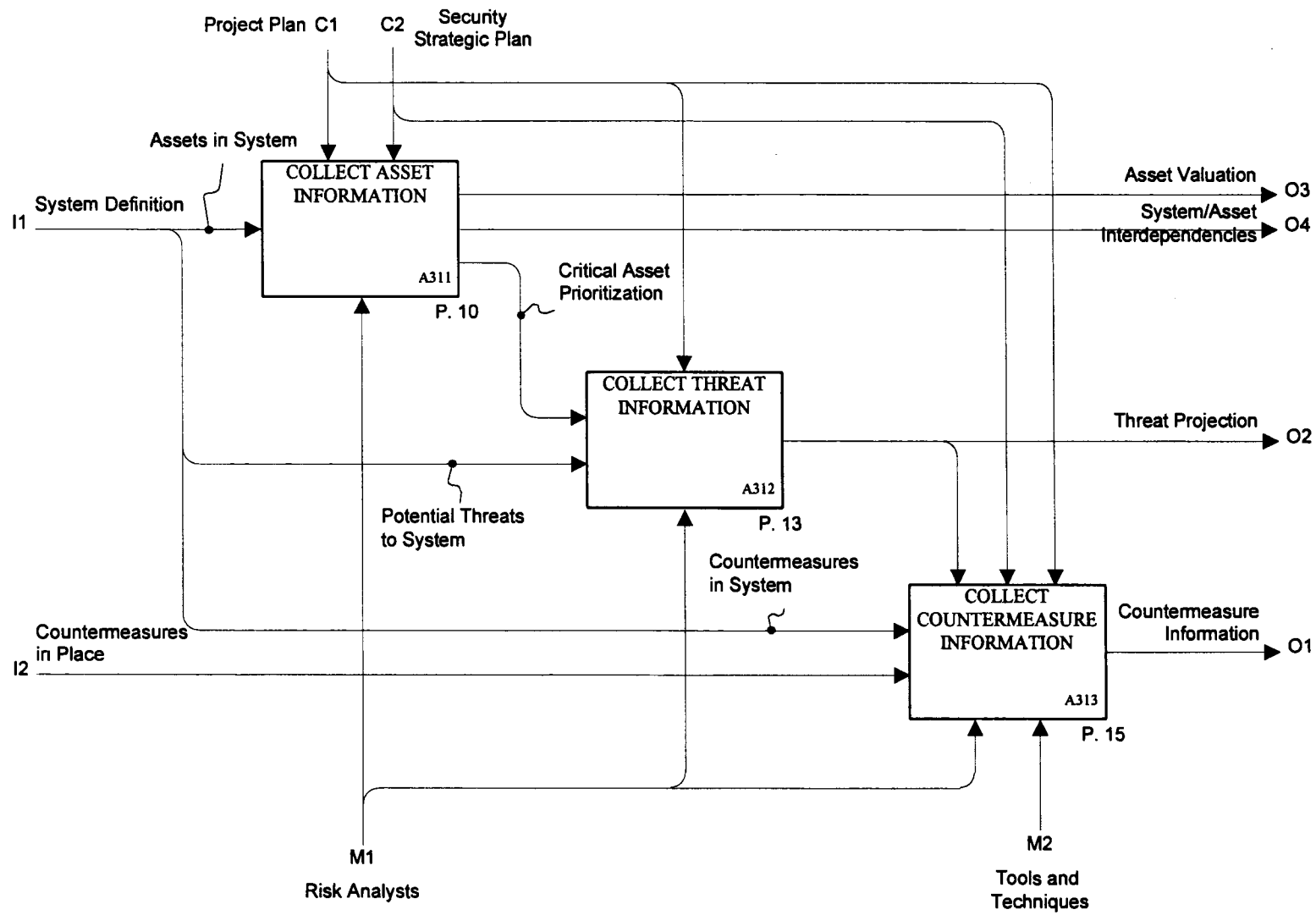
NODE: A24	TITLE: PLAN PROJECT	NUMBER: P. 7

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 06/22/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
	NOTES: 1 2 3 4 5 6 7 8 9 10			RECOMMENDED			
			x	PUBLICATION			



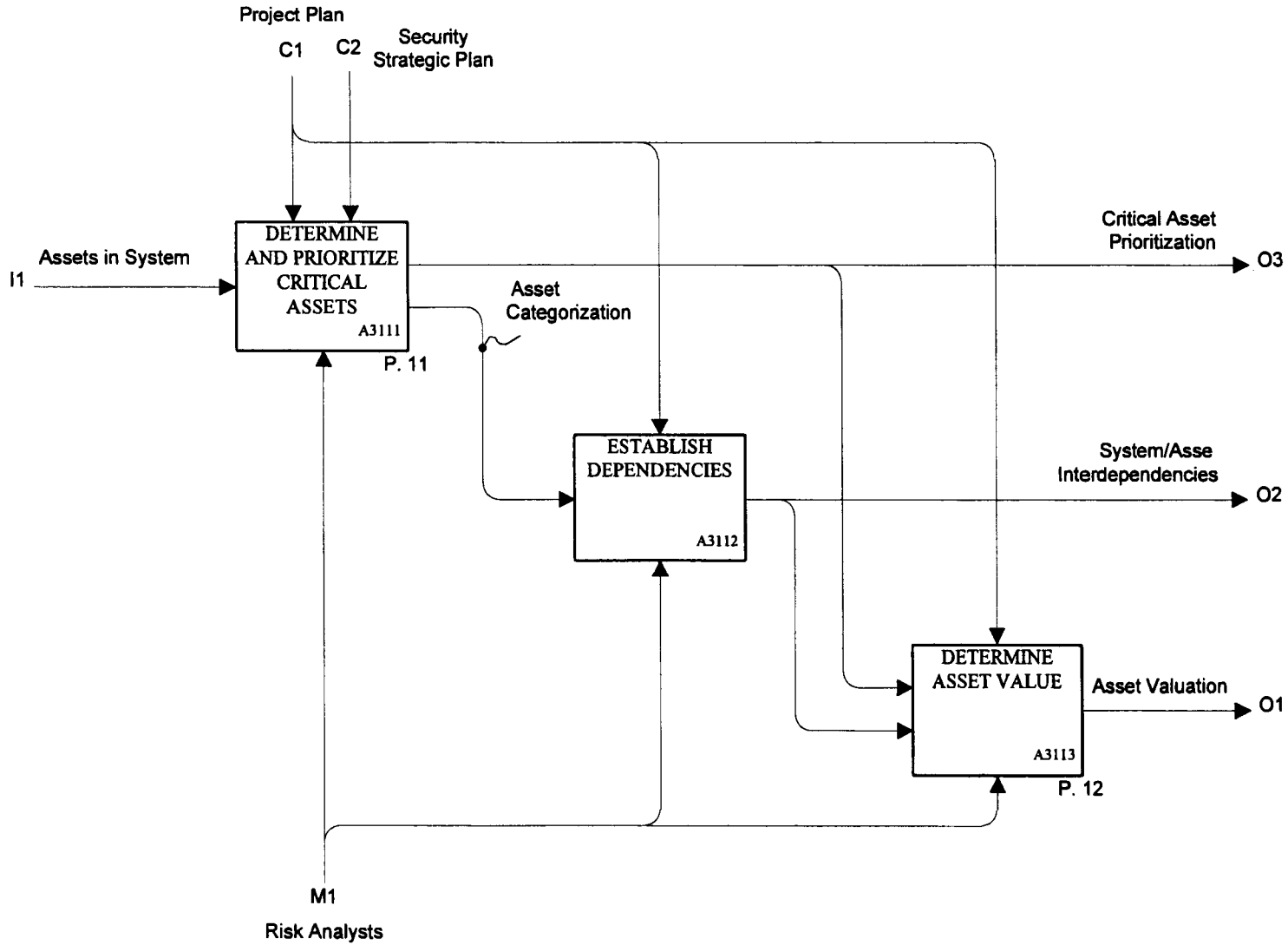
NODE: A3	TITLE: ASSESS RISK	NUMBER: P. 8

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 06/22/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



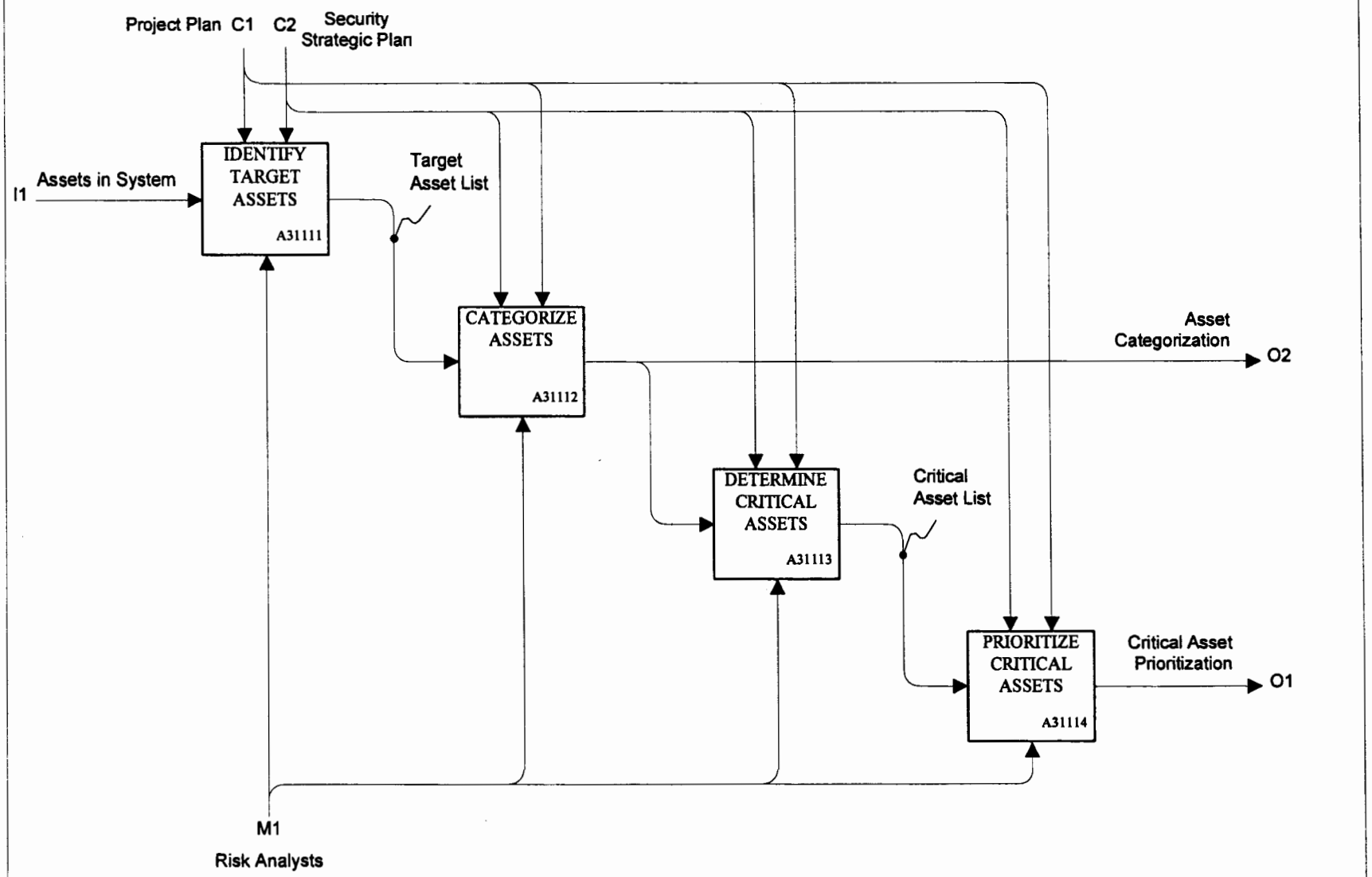
NODE: A31	TITLE: COLLECT DATA	NUMBER: P. 9

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



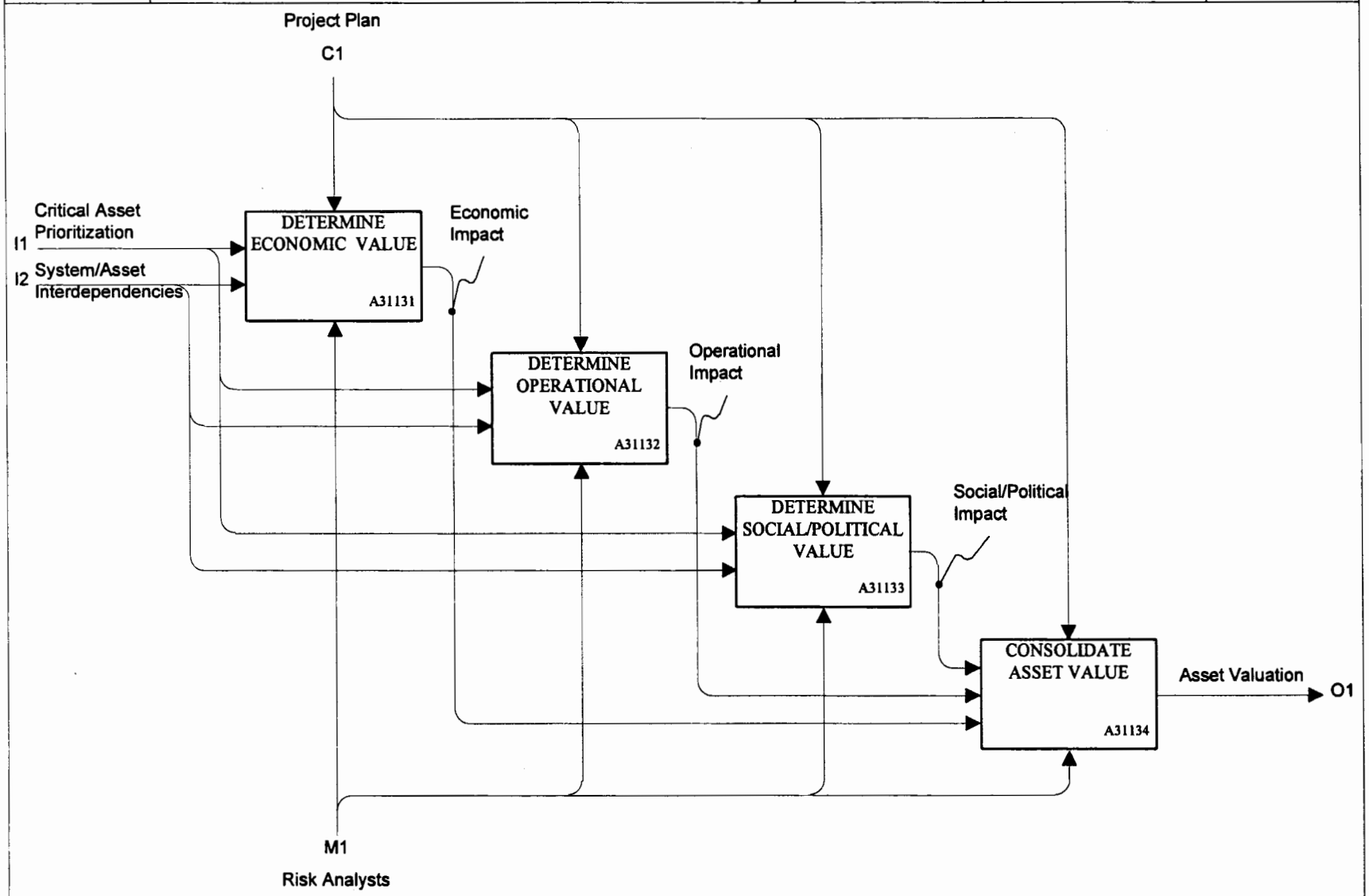
NODE: A311	TITLE: COLLECT ASSET INFORMATION	NUMBER: P. 10

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



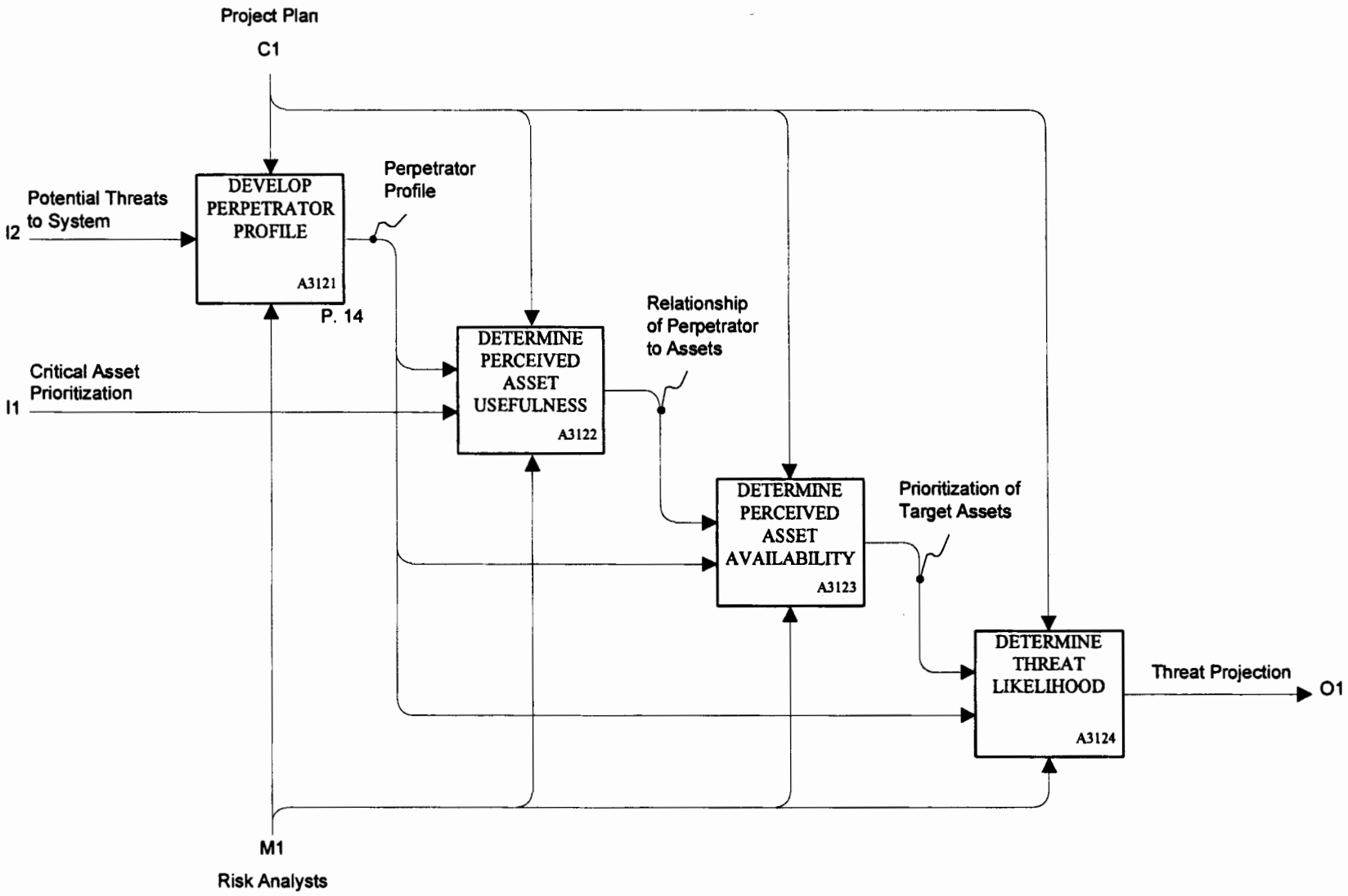
NODE: A3111	TITLE: DETERMINE AND PRIORITIZE CRITICAL ASSETS	NUMBER: P. 11

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



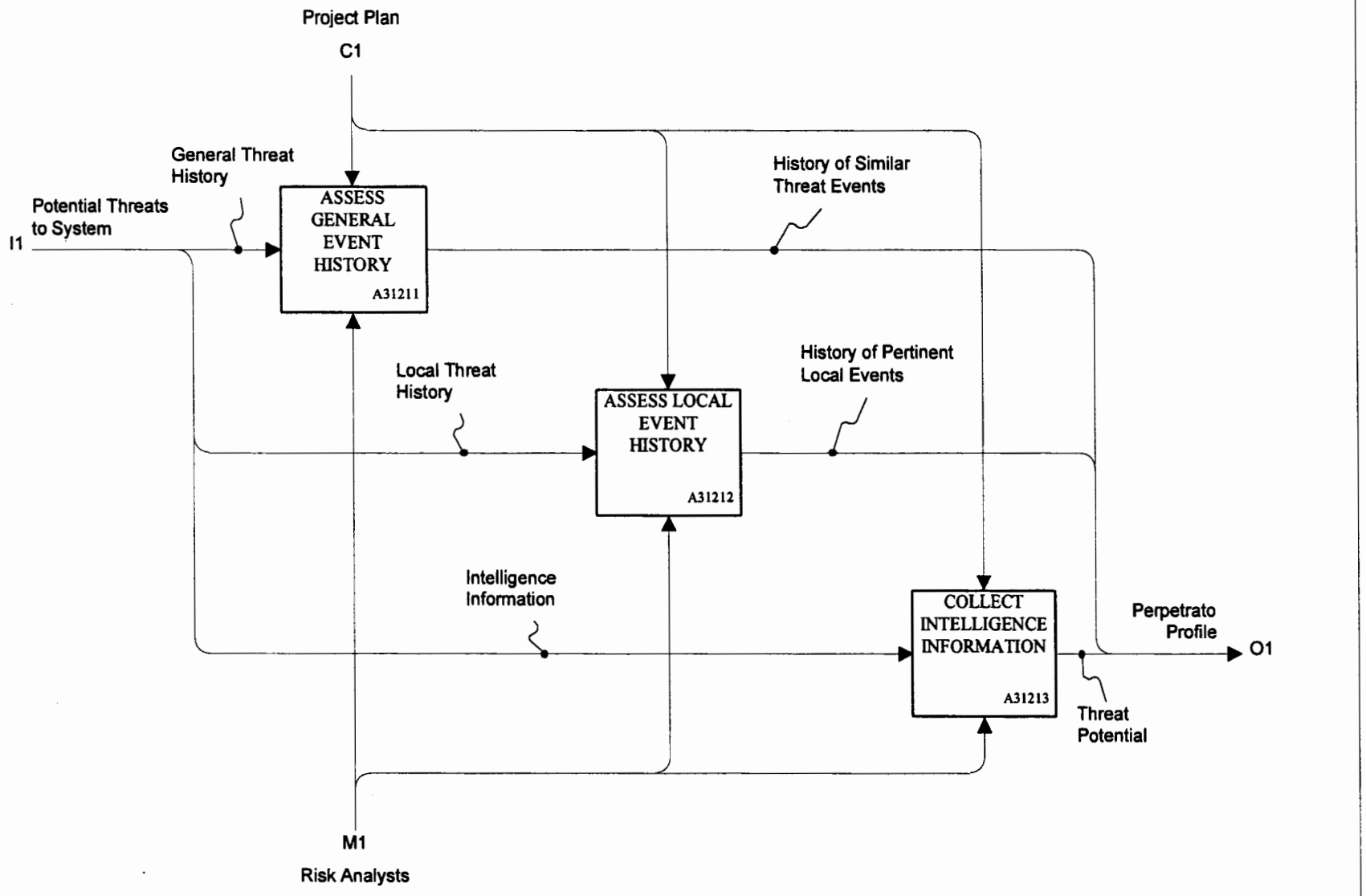
NODE: A3113	TITLE: DETERMINE ASSET VALUE	NUMBER: P. 12

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



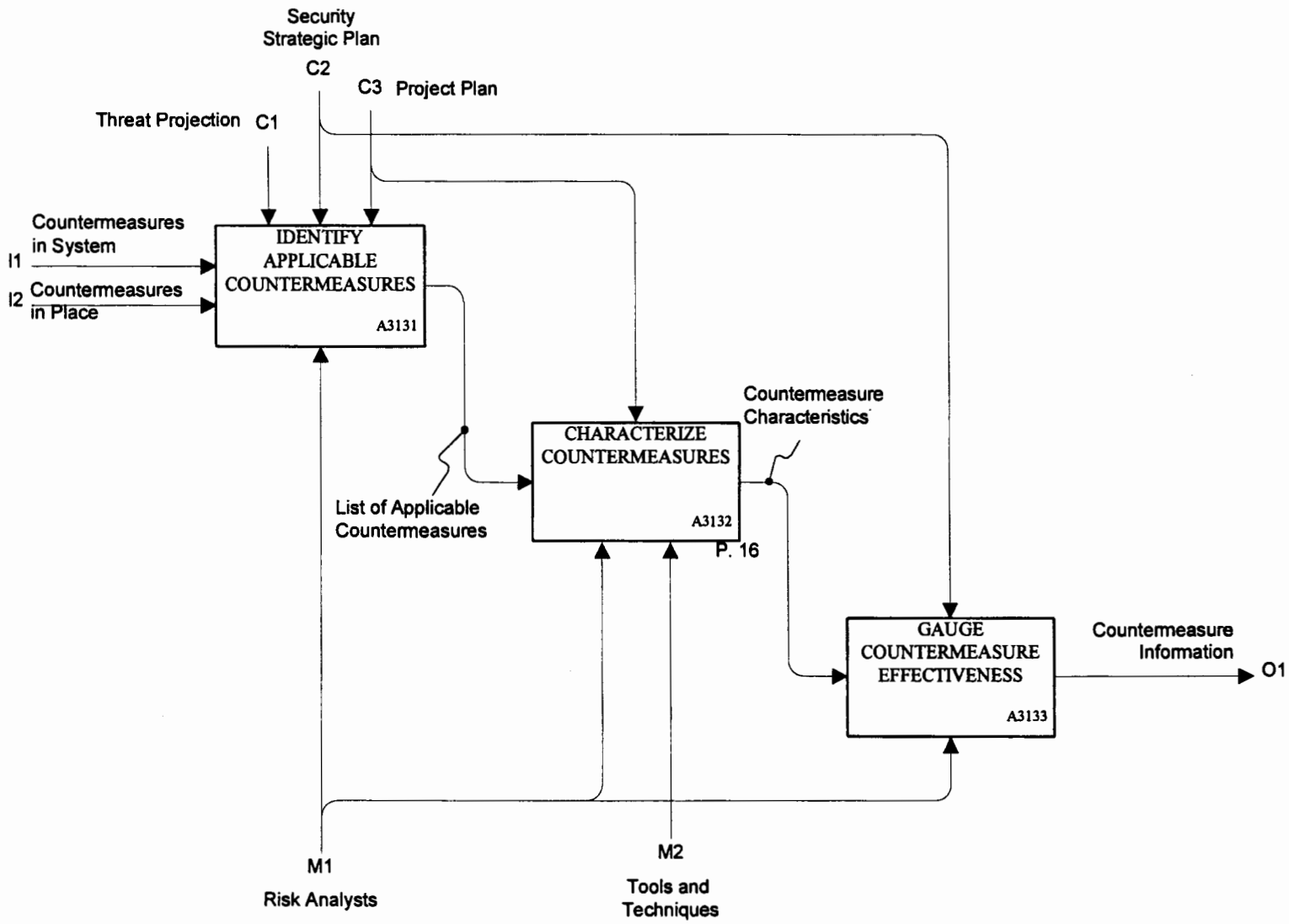
NODE: A312	TITLE: COLLECT THREAT INFORMATION	NUMBER: P. 13

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
	NOTES: 1 2 3 4 5 6 7 8 9 10			RECOMMENDED			
			x	PUBLICATION			



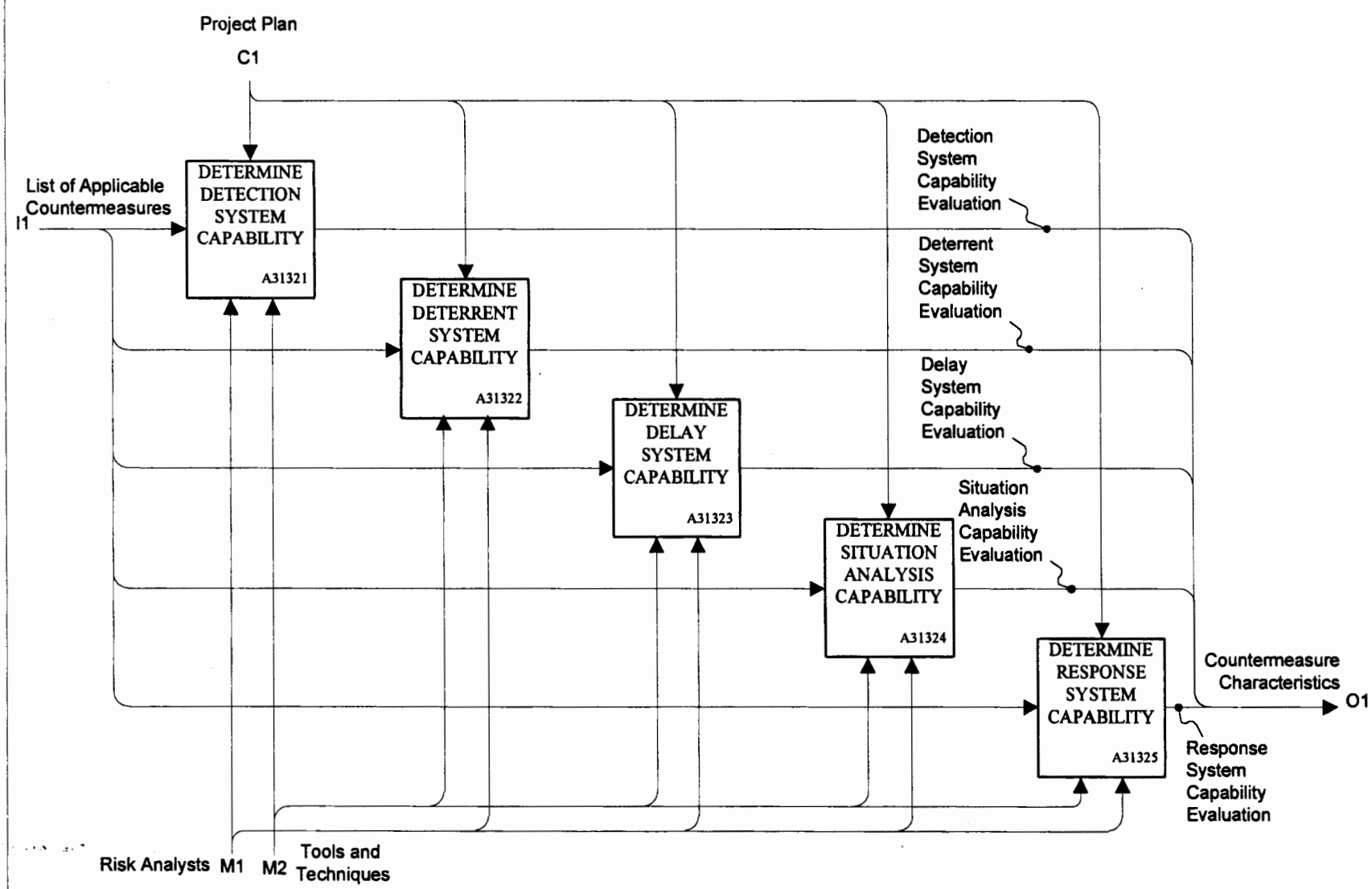
NODE: A3121	TITLE: DEVELOP PERPETRATOR PROFILE	NUMBER: P. 14

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 06/22/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



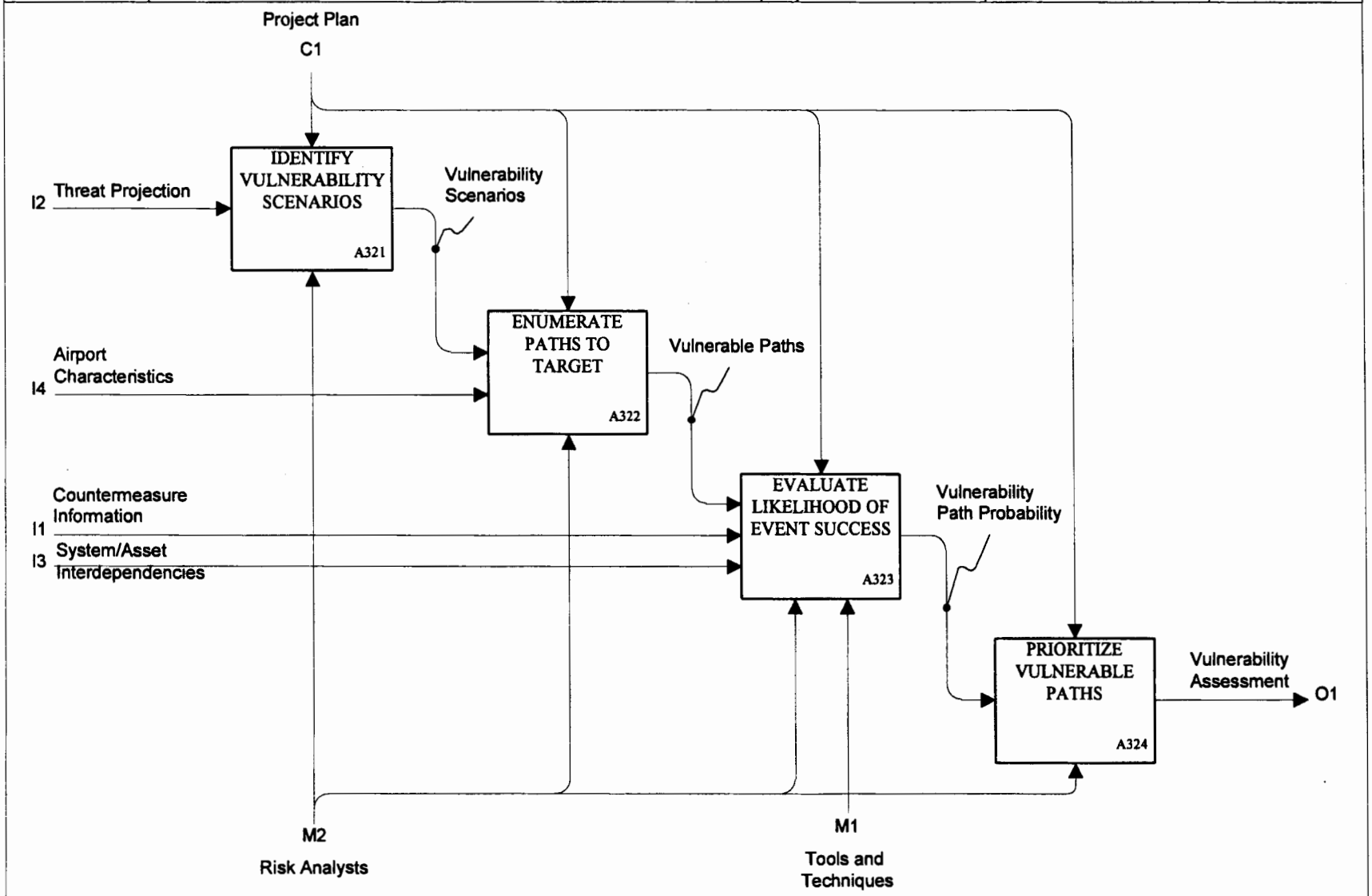
NODE: A313	TITLE: COLLECT COUNTERMEASURE INFORMATION	NUMBER: P. 15

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



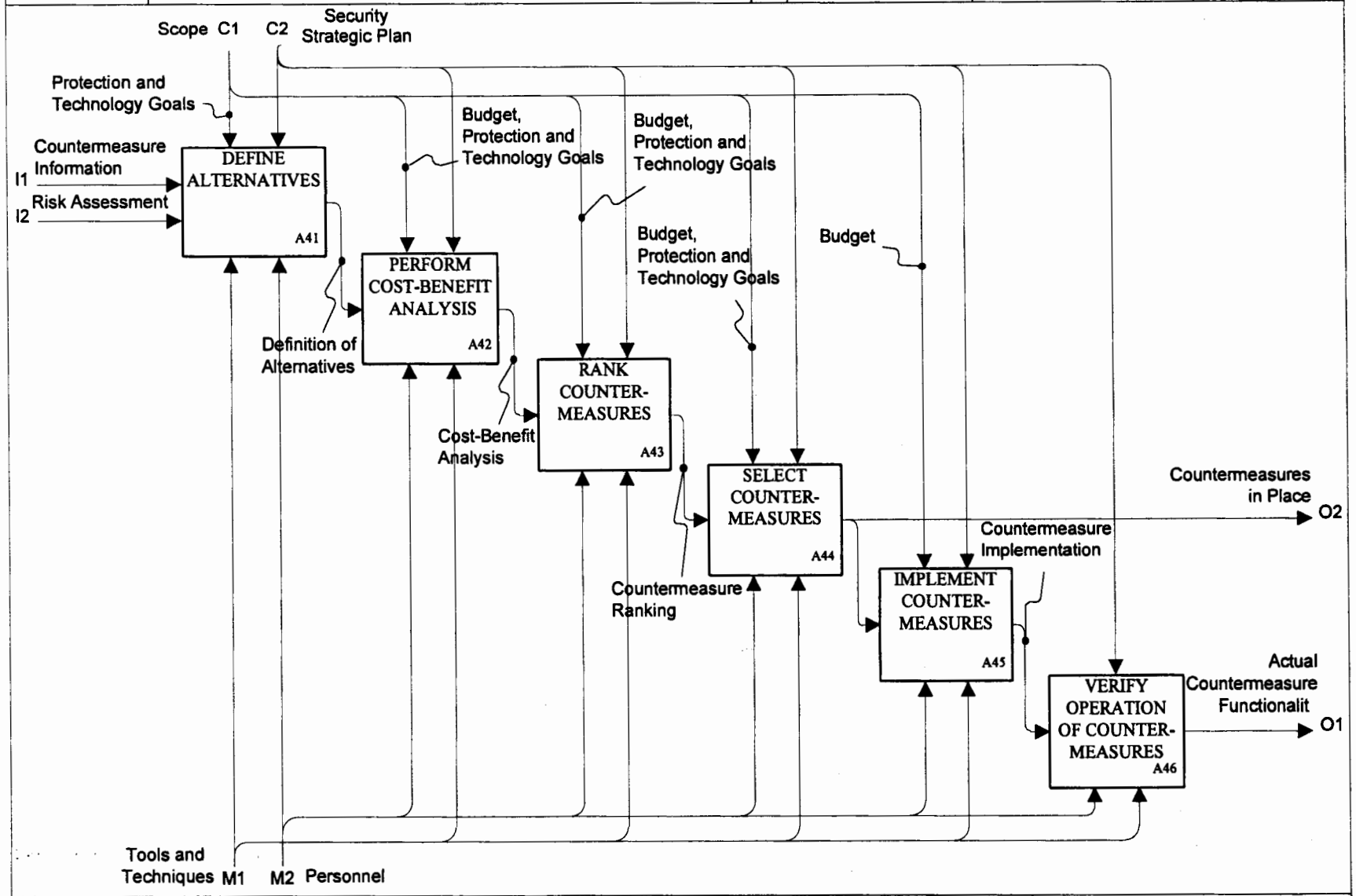
NODE: A3132	TITLE: CHARACTERIZE COUNTERMEASURES	NUMBER: P. 16

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



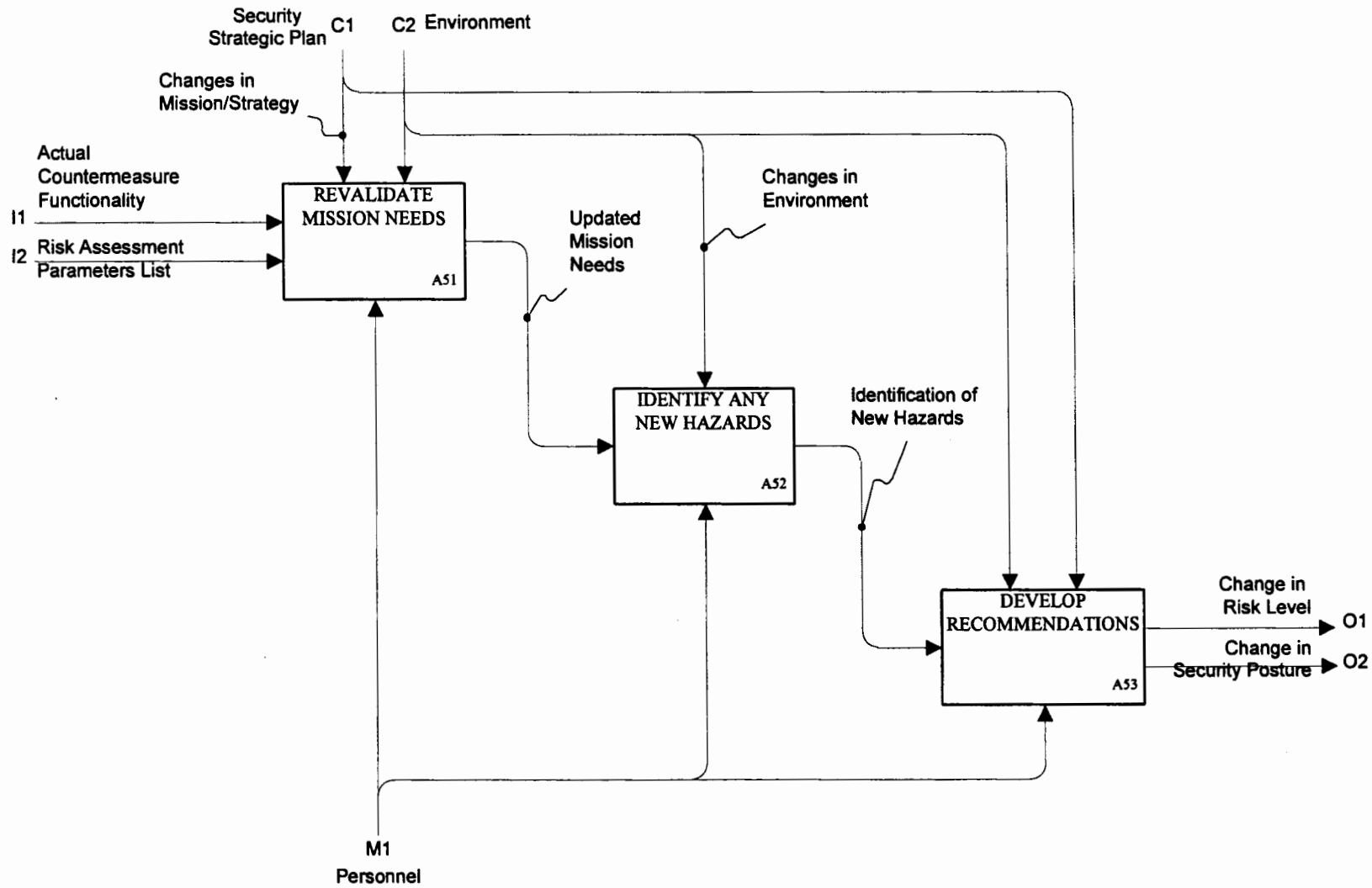
NODE: A32	TITLE: EVALUATE VULNERABILITY	NUMBER: P. 17

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 06/22/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



NODE: A4	TITLE: SELECT AND IMPLEMENT COUNTERMEASURES	NUMBER: P. 18

USED AT:	AUTHOR: Abacus Technology Corporation	DATE: 05/14/99		WORKING	READER	DATE	CONTEXT:
US Commercial Airports	PROJECT: FAATC Risk Management Process	REV:		DRAFT			
				RECOMMENDED			
	NOTES: 1 2 3 4 5 6 7 8 9 10		x	PUBLICATION			



NODE: A5	TITLE: MONITOR COUNTERMEASURE EFFECTIVENESS & CHANGES IN RI...	NUMBER: P. 19

- [A0] MANAGE RISK
  - [A1] ESTABLISH RISK MANAGEMENT STRATEGIC PLAN
    - [A11] ESTABLISH OBJECTIVES
    - [A12] ESTABLISH POLICY
    - [A13] ESTABLISH AUTHORITY AND COORDINATION
  - [A2] FORMULATE APPROACH
    - [A21] DEFINE SCOPE
      - [A211] DETERMINE PROTECTION GOAL
      - [A212] DETERMINE BUDGET
      - [A213] DETERMINE TECHNOLOGY GOALS
    - [A22] DEFINE BOUNDARY
    - [A23] DETERMINE ANALYSIS APPROACH AND TOOLS
      - [A231] IDENTIFY METHODOLOGY
      - [A232] IDENTIFY TOOLS
      - [A233] DEFINE PROCEDURES
    - [A24] PLAN PROJECT
      - [A241] IDENTIFY SKILLS REQUIRED
      - [A242] SELECT TEAM MEMBERS
      - [A243] ESTABLISH SCHEDULE AND MILESTONES
  - [A3] ASSESS RISK
    - [A31] COLLECT DATA
      - [A311] COLLECT ASSET INFORMATION
        - [A3111] DETERMINE AND PRIORITIZE CRITICAL ASSETS
          - [A31111] IDENTIFY TARGET ASSETS
          - [A31112] CATEGORIZE ASSETS
          - [A31113] DETERMINE CRITICAL ASSETS
          - [A31114] PRIORITIZE CRITICAL ASSETS
        - [A3112] ESTABLISH DEPENDENCIES
        - [A3113] DETERMINE ASSET VALUE
          - [A31131] DETERMINE ECONOMIC VALUE
          - [A31132] DETERMINE OPERATIONAL VALUE
          - [A31133] DETERMINE SOCIAL/POLITICAL VALUE
          - [A31134] CONSOLIDATE ASSET VALUE
      - [A312] COLLECT THREAT INFORMATION
        - [A3121] DEVELOP PERPETRATOR PROFILE
          - [A31211] ASSESS GENERAL EVENT HISTORY
          - [A31212] ASSESS LOCAL EVENT HISTORY
          - [A31213] COLLECT INTELLIGENCE INFORMATION
        - [A3122] DETERMINE PERCEIVED ASSET USEFULNESS
        - [A3123] DETERMINE PERCEIVED ASSET AVAILABILITY
        - [A3124] DETERMINE THREAT LIKELIHOOD

[A313] COLLECT COUNTERMEASURE INFORMATION
[A3131] IDENTIFY APPLICABLE COUNTERMEASURES
[A3132] CHARACTERIZE COUNTERMEASURES
[A31321] DETERMINE DETECTION SYSTEM CAPABILITY
[A31322] DETERMINE DETERRENT SYSTEM CAPABILITY
[A31323] DETERMINE DELAY SYSTEM CAPABILITY
[A31324] DETERMINE SITUATION ANALYSIS CAPABILITY
[A31325] DETERMINE RESPONSE SYSTEM CAPABILITY
[A3133] GAUGE COUNTERMEASURE EFFECTIVENESS
[A32] EVALUATE VULNERABILITY
[A321] IDENTIFY VULNERABILITY SCENARIOS
[A322] ENUMERATE PATHS TO TARGET
[A323] EVALUATE LIKELIHOOD OF EVENT SUCCESS
[A324] PRIORITIZE VULNERABLE PATHS
[A33] EVALUATE RISK
[A4] SELECT AND IMPLEMENT COUNTERMEASURES
[A41] DEFINE ALTERNATIVES
[A42] PERFORM COST-BENEFIT ANALYSIS
[A43] RANK COUNTER- MEASURES
[A44] SELECT COUNTER- MEASURES
[A45] IMPLEMENT COUNTER- MEASURES
[A46] VERIFY OPERATION OF COUNTER- MEASURES
[A5] MONITOR COUNTERMEASURE EFFECTIVENESS & CHANGES IN RISK FACTORS
[A51] REVALIDATE MISSION NEEDS
[A52] IDENTIFY ANY NEW HAZARDS
[A53] DEVELOP RECOMMENDATIONS

This page intentionally left blank.

APPENDIX B

GLOSSARY OF TERMS AND CONCEPTS

This page intentionally left blank.

Appendix B: Glossary of Terms and Concepts

This Section presents definitions of risk concepts and the process methodology approach used in the Risk Management Process and discussed in this guide. The Glossary includes general risk and Integrated DEFinition Language (IDEF0) concepts, the primary steps (activities) in the Risk Management Process, and the ICOMs (Inputs, Controls, Outputs, and Mechanisms) of the Risk Management Process.

B1. GENERAL CONCEPTS

This section defines general risk and IDEF0 concepts discussed in this guide.

Boundary – The border or limit of the system defined in the scope.

Context Diagram (A-0 Page) – The representation in an activity model, of the scope, purpose, primary activity, and system boundaries (interfaces) of a process. Everything in the model comes from a decomposition of the context diagram. For the Risk Management Process, the Context Diagram reflects the activity Risk Management and its interfaces.

Decomposition of an IDEF Model – The representation in an IDEF0 model of a subordinate process to the Context Diagram or any subsequent process step.

Environment – The external circumstances, conditions, and characteristics that affect the existence and development of the system.

ICOM – An acronym used in IDEF0 Modeling to denote Inputs, Controls, Outputs, and Mechanisms.

Integration DEFinition Language 0 (IDEF0) – A process modeling methodology used to model a wide variety of automated and non-automated systems.

Methodology – In a process step, a technique or procedure for accomplishing the activity of the process.

Node Index – An indented listing showing nodes particular system activities, in an IDEF0 model in "outline" order.

Process – A repeatable, well-defined, and tested set of procedures for accomplishing a complex task.

Process Step – A discrete and highly defined action, carried out by a machine, personnel, or a combination, that accomplishes a specific activity within a process.

Risk – An expression of the probability and impact of an undesired event in terms of event severity and event likelihood.

System – A group of interrelated, interacting, or interdependent components in a universe forming a complex whole, to accomplish a mission.

Universe – All existing systems and conditions.

Vulnerability – Weaknesses or flaws in a system that may conceivably be exploited by a threat.

Vulnerability Scenario – The combination of an associated perpetrator, threat device, and target which may compromise a target asset within a system.

B2. RISK MANAGEMENT PROCESS STEPS

This section describes each of the process steps in the Risk Management Process. The steps, or IDEF0 activities, are listed in order of appearance in the IDEF0 representation, i.e., Node Index, of the Risk Management Process with the IDEF0 reference following in parentheses, e.g., "(Activity A321)."

Risk Management (Activity A0) – The process whereby a security strategic plan is established, an approach formulated, risks assessed, countermeasures implemented and selected, and countermeasure effectiveness and changes in risk assessment factors monitored.

Establish Risk Management Strategic Plan (Activity A1) – Institute established objectives, policy, authority, and coordination to direct the risk management process.

Establish Objectives (Activity A11) – To set goals toward achieving the system's strategic mission.

Establish Policy (Activity A12) – To implement procedures and guidelines for achieving the system's strategic mission.

Establish Authority and Coordination (Activity A13) – To establish authority and chain-of-command for achieving strategic objectives and implementing security policy.

Formulate Approach (Activity A2) – To establish a formal statement of risk assessment performance by defining the scope and the boundary, and selecting risk analysis methodology and planning for the project.

Define Scope (Activity A21) – To determine the extent of the area or aspects of the universe that are covered in the risk management process by determining a protection goal, budget, and technological goals.

Determine Protection Goal (Activity A211) – To decide the ultimate goal of the risk assessment, while acknowledging and accepting the remainder of any risk.

Determine Budget (Activity A212) – To determine the financial scope by developing a plan for adjusting expenditures to income, producing budgetary guidelines.

Determine Technology Goals (Activity A213) – To determine the objectives applying science and industrial technical advances, while meeting budgetary guidelines.

Define Boundary (Activity A22) – To determine the extent of the dividing line between the system and the environment.

Determine Analysis Approach and Tools (Activity A23) – To select the processes and procedures utilized in an analysis of system assets and vulnerabilities in order to establish an expected loss from threat events based upon estimated probabilities of the occurrence of these events.

Identify Methodology (Activity A231) – To select the data collection, vulnerability analysis, and risk analysis processes utilized in an analysis of system assets and vulnerabilities.

Identify Tools (Activity A232) – To select the software used to automate the performance of procedures or steps in the process.

Define Procedures (Activity A233) – To establish the systems and techniques to be used to accomplish each step in the process.

Plan Project (Activity A24) – To plot the course of action and produce a project plan which identifies the skills required, selects team members, and establishes a schedule and milestones for a risk management project.

Identify Skills Required (Activity A241) – To distinguish the proficiencies necessary to carry out various risk management procedures.

Select Team Members (Activity A242) – To identify a group of individuals who posses the skills required to complete the project outlined, producing the team composition.

Establish Schedule and Milestones (Activity A243) – To establish an action plan, which schedules important events projected during the period specified for the project.

Assess Risk (Activity A3) – To evaluate the trade-offs in cost and effectiveness of various countermeasure options and a measurement of residual risk.

Collect Data (Activity A31) – To collect asset information, threat information, and countermeasure information.

Collect Asset Information (Activity A311) – To determine and prioritize critical assets, establish dependencies and determine asset value while assembling the facts and knowledge from objects/items of value (tangible or intangible).

Determine and Prioritize Critical Assets (Activity A3111) – To identify target assets, categorize assets, determine critical assets, and prioritize critical assets into an asset categorization system.

Identify Target Assets (Activity A31111) – To identify the property or effects to protect within a system which, if compromised, may jeopardize the achievement of the system's mission.

Categorize Assets (Activity A31112) – To identify the role of each asset in the system and group them according to their type and/or affect on the system's mission.

Determine Critical Assets (Activity A31113) – To determine which categories of assets are the most crucial to the system's mission.

Prioritize Critical Assets (Activity A31114) – To determine which assets are critical to the system's operations or which have high public visibility (and therefore political impact).

Establish Dependencies (Activity A3112) – To determine which assets from the asset categorization are contingent upon other identified assets in the performance of the system's mission.

Determine Asset Value (Activity A3113) – To determine the worth of property or effects from the chosen system.

Determine Economic Value (Activity A31131) – To determine the potential economic loss due to the damage or destruction of an asset in the system.

Determine Operational Value (Activity A31132) – Determine the effect on the system's operations due to damage or destruction of its assets.

Determine Social/Political Value (Activity A31133) – To determine indirect value of the damage or loss of a target asset in terms of degradation in reputation or customer confidence.

Consolidate Asset Value (Activity A31134) – To combine and unite the value of the assets selected from the system.

Collect Threat Information (Activity A312) – To assemble facts and information regarding potential perpetrators from both the system and collected asset information.

Develop Perpetrator Profile (Activity A3121) – To illustrate the striking characteristics of potential aggressors in the form of a biographical sketch.

Assess General Event History (Activity A31211) – To evaluate contingent situations relating to incidents which have occurred in the past.

Assess Local Event History (Activity A31212) – To evaluate the restricted characteristics of past events pertaining to the system.

Collect Intelligence Information (Activity A31213) – To collect secret information in order to disclose any potential threats and/or perpetrator profile.

Determine Perceived Asset Usefulness (Activity A3122) – To determine which assets may be advantageous to compromise in the pursuit of a potential perpetrator's goals.

Determine Perceived Asset Availability (Activity A3123) – To determine which assets are accessible to the potential perpetrator.

Determine Threat Likelihood (Activity A3124) – To determine the probability of occurrence of a threat event.

Collect Countermeasure Information (Activity A313) – To group countermeasure information by identifying applicable countermeasures, characterizing countermeasures, and measuring countermeasure effectiveness.

Identify Applicable Countermeasures (Activity A3131) – To discern which safeguards protect the system's critical assets.

Characterize Countermeasures (Activity A3132) – To describe the features of countermeasures by determining the following: detection system capability, deterrent system capability, delay system capability, situation analysis capability and response system capability.

Determine Detection System Capability (Activity A31321) – To determine the system's ability to perceive or discern threats.

Determine Deterrent System Capability (Activity A31322) – To determine the system's ability to prevent or discourage threats.

Determine Delay System Capability (Activity A31323) – To determine the system's ability to experience a deferment and the potential longevity of such a delay.

Determine Situation Analysis Capability (Activity A31324) – To determine the effectiveness of the elements used to characterize the countermeasures.

Determine Response System Capability (Activity A31325) – To determine the system's reaction capability in relation to the list of applicable countermeasures.

Gauge Countermeasure Effectiveness (Activity A3133) – To measure the effectiveness if safeguards against possible threats as part of collecting countermeasure information.

Evaluate Vulnerability (Activity A32) – To evaluate the system characteristics to determine any weaknesses which may be exploited by a threat.

Identify Vulnerability Scenarios (Activity A321) – To identify those scenarios in which a target asset within the system may be compromised by a perpetrator and threat device.

Enumerate Paths to Target (Activity A322) – To list the potential courses followed to achieve a perpetrator's vulnerability objectives.

Evaluate the Likelihood of Event Success (Activity A323) – To assess the probability that the perpetrator will achieve his or her goal along a particular path.

Prioritize Vulnerable Paths (Activity A324) – Rank vulnerable paths according to the likelihood that the perpetrator will achieve his or her goal along a particular path.

Select and Implement Countermeasures (Activity A4) – To choose among and execute the recommendations for safeguards identified through the risk management process.

Define Alternatives (Activity A41) – To identify all currently available safeguards and planned technologies that would mitigate the recognized vulnerabilities and risks in the system.

Perform Cost-Benefit Analysis (Activity A42) – To compare the costs of safeguards with the reduction in risk they accomplish.

Rank Countermeasures (Activity A43) – To list safeguards according to a methodology representing the reduction in risk they accomplish versus their cost.

Select Countermeasures (Activity A44) – To choose safeguards which accomplish the greatest combined reduction in risk within the available budget.

Implement Countermeasures (Activity A45) – To put the selected countermeasures in place.

Verify Operation of Countermeasures (Activity A46) – To confirm that implemented countermeasures perform to their expected capacity once operational.

Monitor Countermeasure Effectiveness and Changes in Risk Factors (Activity A5) – To continually evaluate the threat situation and review baseline data to consider new assets, construction impacts, newly uncovered vulnerabilities, or other changes in the system.

Revalidate Mission Needs (Activity A51) – To confirm the strategic objects of the system.

Identify Any New Hazards (Activity A52) – To identify changes in the system and its environment that produce additional risks to the system.

Develop Recommendations (Activity A53) – To suggest a course of action based on a review of risk factors in the system.

B3. ICOMS

This section defines the high-level Risk Management Process activity interfaces, i.e., Inputs, Controls, Outputs, and Mechanisms. The ICOMS are presented alphabetically, as they may appear more than once in the process, e.g., the Output of one activity becomes the Input to another.

Acceptance of Residual Risk (ICOM) – Acceptance of the reminding expression of the probability and impact of an undesired event in terms of event severity and event likelihood.

Actual Countermeasure Functionality (ICOM) – An actual physical device, person, procedure, or combination of one or more of these intended to reduce or eliminate one or more identified vulnerabilities.

Affected Parties (ICOM) – Individuals and organizations acted upon by the environment or influenced, favorably or adversely, by proposed risk management actions and decisions.

Analysis Approach (ICOM) – The processes and procedures utilized in a study of system assets and vulnerabilities in order to establish an expected loss from threat events based upon estimated probabilities of the occurrence of these events.

Boundary (ICOM) – The border or limit of the system defined in the scope.

Changes in Risk Level (ICOM) – Change in the circumstances, conditions, vulnerabilities, and countermeasures that affect the initial risk level of a system.

Changes in Security Posture (ICOM) – Change in the external circumstances, conditions, and that affect the existence and development of the security of the system.

Cost-Benefit Analysis (ICOM) – The process of comparing the costs of safeguards with the reduction in risk they accomplish.

Countermeasures in Place (ICOM) – The countermeasures established in a system.

Environment (ICOM) – The external circumstances, conditions, and characteristics that affect the existence and development of the system.

Initial Risk Level (ICOM) – Risk as measured at the starting point of the process.

Management (ICOM) – The personnel responsible for directing the operation of the system.

Organizational Mission (ICOM) – The operational function and associated roles and responsibilities of a system.

Project Plan (ICOM) – A plan, determining the protection goal, budget, and technology goals using risk analysis procedures.

DOT/FAA AR-99/94 **Guide to the FAATC risk management process**
C. 2
00021436
Tech Center Library

Risk Analysis Methodology (ICOM) – The data collection, vulnerability analysis, and risk analysis processes utilized in an analysis of system assets and vulnerabilities.

Risk Analysts (ICOM) – The personnel responsible for conducting and maintaining the risk assessment(s) of a system.

Risk Assessment (ICOM) – A document that describes risk events, and an estimation of the likelihood and impact of the occurrence of such events.

Scope (ICOM) – The delineation of level of effort, areas of the universe the systems, and boundaries of that are covered in the vulnerability assessment process.

Security Strategic Plan (ICOM) – The statement of security objectives, policy, and associated roles and responsibilities of a system.

System Definition (ICOM) – The delineation of a group of interrelated, interacting, or interdependent components forming a complex whole to accomplish a particular mission.

Technology Goals (ICOM) – The objectives in applying science and industrial technical advances.

Threat Projection (ICOM) – The assessment of the capability of an adversary, coupled with his intentions as declared by words or action, to undertake any activity detrimental to the success of a system, program, activities or operations, or to a property and human life.

Tools and Techniques (ICOM) – ***Tools*** are software implementations of a set of techniques to automate the performance of many procedures or steps in the process. ***Techniques*** are the systematic procedures by which each step in the process is accomplished.

Vulnerability Assessment (ICOM) – The identification of assets and their level of exposure to specific threat vectors due to the inability of existing countermeasures to protect them.