Unemployment Insurance Service
Risk Analysis User's Guide

Step-By-Step Approach
For
State Employment Security Agencies
Featuring RiskWatch® Software

U.S. Department of Labor
Employment and Training Administration

August 1999

TABLE OF CONTENTS

Preface

Purpose

The Risk Analysis User's Guide is UI specific and the product of a Federal-State workgroup. The guide's intent is to assist the analyst's critical thinking skills and decision-making processes regarding the different methods of performing a risk analysis. Additionally, the guide will assist the State Employment Security Agencies in conducting their risk analyses using the software package, RiskWatch®, without specialized contractor assistance. Also, the guide will provide a consistent review of the risk analysis process at each SESA. SESAs may use any automated risk analysis software package, such as RiskWatch®, to perform their risk analysis.

Scope of the Manual/Guide

The User's Guide discusses general risk analysis theory and the application of the RiskWatch software in applying that theory.

Assumptions

The User Guide assumes that the analyst is using RiskWatch® version 7.1 Basic. It also assumes that the analyst is familiar with Windows 3.xx or above.

Disclaimers

Using the Risk Analysis User's Guide is not intended to be the best or only way to conduct a risk analysis. As RiskWatch® introduces new versions of the software, some of the procedures outlined in this manual may become obsolete, superfluous, or otherwise unnecessary because of technical advances.

Formatting

The format for the guide is as follows:

- Bulleted items relate to risk analysis theory and RiskWatch® standard precepts.

1. Numbered items are processes to be completed or represent a step by step input.

The boxes and pictures are as followed:

EXAMPLE is red box with blue text.

TIP is green box with pink text.

WARNING is yellow box with red text.

Theory

RiskWatch®

Workgroup Members

Nancy Edmunds	State of Nebraska
August Matlock	State of Missouri
Rebecca Morales	State of California
Paul Riley	State of Alabama
Colleen Scow	State of Montana
John Stanley	State of Indiana
Harry Minor	Department of Labor

This page left blank intentionally.

Introduction To Risk Analysis

What is a Risk Analysis?

A risk analysis is an application of a standardized methodology in the determination of threats, risk factors, vulnerability exposures, and potential losses. Risk Analysis is an approach to satisfying the need of an organization to protect the assets in which it has made an investment. The risk analysis also serves to identify the particular problems an organization could expect to encounter in the performance of its MISSION, and the adverse effects these problems might present to the organization's ability to meet its obligations. A risk analysis is a mechanism by which management can address these problems according to their relative importance based on financial analysis, and to develop safeguards which are both reasonable and cost-effective. It addresses four main components:

- Valuation of ASSETS
- Measurement of VULNERABILITY
- Impact of THREATS
- Effectiveness of SAFEGUARDS

Risk Analysis is not an exact science. However, it can be expressed as a mathematical equation:

ASSET x VULNERABILITY x THREAT = RISK
RISK is then reduced by the effectiveness of SAFEGUARDS

How is Risk Analysis Defined?

Risk analysis provides a method to:

- Determine threats, risk factors, vulnerability exposures, and potential losses.
- Satisfy an organization's need to protect the assets in which it has invested.
- Identify the threats that an organization could encounter in performing its mission and the consequences these threats present to the organization's ability to meet its mission.

Why Should A Risk Analysis Be Performed?

- To meet Federal Requirements (UIPL 34-87)
- To identify new or increased vulnerabilities associated with system changes (new or major)
- As a prerequisite to Disaster Recovery Planning

What Are The Benefits?

- Increased security awareness.
- A quantitative measure of the level of risk.
- Vulnerabilities ranked in order of non-compliance.
- Safeguards ranked according to the best Return On Investment (ROI).
- Management tool to provide information to support management decisions.
- Reduced Losses
- Protected Assets

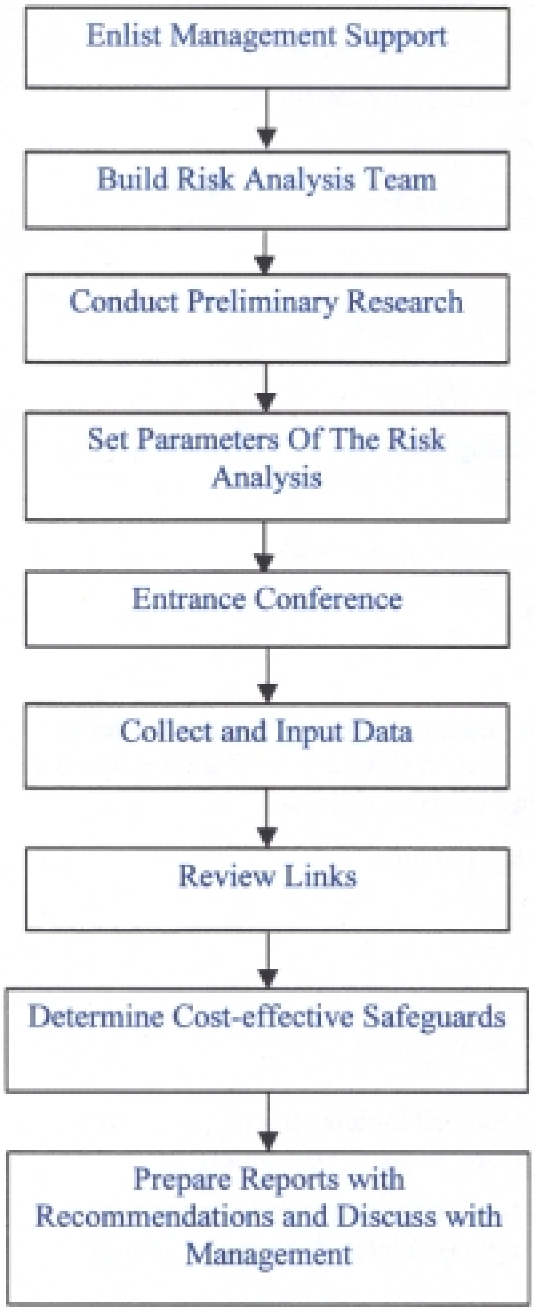
What Does the Risk Analysis Process Include?

- Identifying assets and determining their value;
- Identifying the threats that adversely affect assets;
- Determining the means and frequency of threats;
- Identifying safeguards to reduce the likelihood of threats; and,
- Determining a plan to select and implement cost-effective safeguards.

Explanation of the Risk Analysis Process

The flowchart below provides a basic outline of the overall risk analysis process. Following the flowchart, each process step is briefly explained.

Risk Analysis Flowchart


Enlist Management Support
Build Risk Analysis Team
Conduct Preliminary Research
Set Parameters Of The Risk Analysis
Entrance Conference
Collect and Input Data
Review Links
Determine Cost-effective Safeguards
Prepare Reports with Recommendations and Discuss with Management

Enlisting Support

- Make a formal presentation to top level management
  - Explain the importance of the risk analysis
  - Sample Memo Announcing Review on page 184
  - Use media examples
- Management must delegate authority and delineate purpose/scope
  - Sample Memo from Executive to Unit(s) under Review on page 185
  - Optional: "Statement of Understanding"
    - Sample Statement of Understanding on page 190

Build Risk Analysis Team

- Analyst(s)- Risk analysis project leader
- Internal Consultant(s) - Business function expert(s)
- Encourage input and involvement from all disciplines
- Desirable individual / team attributes
  - Broad scope of knowledge of the department's operations
  - Established network within the department

Conduct Preliminary Research

To provide the Analyst/RiskWatch user with basic knowledge of the business function under analysis and the RiskWatch software, the analyst should collect and review the following information prior to actually beginning the risk analysis.

- High level flow charts of the selected business function.
- Organization Chart(s)
- Existing, relevant policies and procedures
- Existing inventory lists
- Walk-through of the business function
- Interviews with appropriate personnel (e.g., financial management, program experts, information technology (IT) staff, users, security personnel)
- Walk-through RiskWatch using a "dummy" case to become familiar with the software's screens and layout. Refer to Using RiskWatch A Step-By-Step Approach.
- RiskWatch printouts and information from (e.g., question sets, category definitions)

- Unemployment Insurance risk analysis questions created from *"Potential Current and Future Vulnerabilities"*, March 1997. Each SESA received these questions on disk for import into RiskWatch. Refer to Section 6 of this guide for the Question Phase on how to Import UINRAP Questions Category.

Set the Parameters of the Risk Analysis

- Consider the following when setting parameters for the analysis and in RiskWatch
  - Define the risk analysis subject (i.e. business function, process, system, etc)
  - Establish the start and end points of the subject.
  - Define and list assumptions for use throughout the study. For example:
    - Staffing resources and business functions will not change.
    - Purpose to exclude certain threats (e.g. Y2K)
  - Define and list any constraints.
  - Define the functions, entities, systems, etc., associated with the subject.
- Propose the risk analysis parameters to executive management.

> TIP
> Advisable To Limit Scope To A Manageable Size

Entrance Conference

- Introduce the purpose, plan, and benefits of the risk analysis with business function management.
- Define involvement of management and staff :
  - Announce plan
    - Sample Proposal To Conduct Risk Analysis on page 188
  - Require full participation
  - Delegate authority
  - Milestones

Collecting and Inputting Data

At this point, the analyst has executive support and a ***basic*** understanding of the business function and RiskWatch software. The analyst now collects detailed information about the business function for input into RiskWatch. Specifically, the analyst collects the information to:

- Identify and value assets.
- Identify potential, relevant threats and vulnerabilities.

- Identify threat annual frequencies.
- Select the appropriate questions and respondents to assess the vulnerability level.
- Determine the adequacy and cost of internal controls (a.k.a. safeguards).

Detailed instruction on where, what, and how to collect and organize data is provided in Section 4, Ideas For Collecting and Organizing Data beginning on page 15. Section 5 Using RiskWatch A Step-By-Step Approach, beginning on page 37, provides instructions on how to input data.

Review Links

RiskWatch creates links between loss, asset, threat and vulnerability categories. The only action required from the analyst is to review the relationships. Links and input data calculate the Annual Loss Expectancy (ALE) and perform the safeguard evaluation.

Determine Cost-Effective Safeguards

The goal of the safeguard is to reduce the Annual Loss Expectancy (ALE) of one or more incidents, thereby reducing the overall ALE for the enterprise. This reduction is calculated by noticing that various safeguards impact the overall system in different ways including recovery, preventative and reduction.

The analyst identifies all safeguards, those existing and those not yet implemented. The degree to which each safeguard may or may not already be implemented can be derived from the responses to the questionnaires, in each area of vulnerability. That pertains to a particular safeguard.

The cost effectiveness of a safeguard is based on the overall cost of the safeguard and the ability of the safeguard to reduce vulnerabilities.

Prepare Reports with Recommendations and Discuss with Management

RiskWatch produces reports, which include numerous graphs. We recommend the user customize these reports to their agency's needs.

Overview Of The RiskWatch® Process

This section introduces the analyst to the process followed by the RiskWatch® software. RiskWatch® uses a series of five (5) phases, which include:

- Phase I – Selection
- Phase II – Data
- Question Phase
- Phase III – Links/Execution
- Phase IV – Reports

The proceeding text provides a brief explanation of each phase, the tasks and data requirements associated with it, and suggestions relevant to completing the phase. Detailed step-by-step instructions are provided in Section 5, Using RiskWatch A Step-By-Step Approach.

Phase I - Selection

In this phase, the analyst defines the following six areas: Functional Areas, Loss Categories, Asset Categories, Threat Categories, Vulnerability Areas, and Safeguard Categories. Below is an explanation of each area. Refer to Appendix C for the definitions of the categories in all six areas.

Functional Areas

The Functional Areas list the different positions personnel may hold in an agency. When a respondent is paired up with a Functional Area, s/he receives all of the questions linked to that function. The analyst can choose one or all of the RiskWatch Functional Areas or create additional functional areas tailored to the agency or business function.

Loss Categories

A loss results from the realization of a threat that causes a decrease in the amount, magnitude, or degree of an asset's value, integrity, availability, or confidentiality. RiskWatch allows the user to select from six loss categories. Select the categories appropriate to the agency or business function.

- Delay/Denial
- Direct Loss
- Disclosure
- Intangibles
- Modification
- Related Direct Loss

Asset Categories

Assets include items of value that an agency uses to accomplish its mission. These assets include tangible (i.e., physical) or intangible (i.e., abstract) items. Tangible items include those assets necessary for a system, function, or entity to perform its normal day-to-day operations or critical business functions. Intangible assets include items such as good will, public trust, and reputation. RiskWatch allows the user to select the asset categories pertinent to the agency or business function from the 21 listed asset categories by deselecting inappropriate categories. New categories cannot be added. The analyst assigns each identified asset during data collection process to one of these asset categories.

Threats

A threat is any potential human or natural event, process, act, or substance that results in a loss to an asset's availability, integrity, or confidentiality. Threats are always present. Examples include:

- Earthquakes,
- Errors,
- Fires,
- Sabotage, or
- Modification of documents or databases.

RiskWatch allows the user to select from 37 threats. Select those appropriate to the agency or business function. RiskWatch requires the user to select the pertinent threats to the agency or business function by deselecting the inappropriate threats. New threats cannot be added. If no threats are deselected, RiskWatch includes all threats in the case.

> TIP
> The Project Team suggests deselecting the Currency Fluctuation and Inflation threat categories, as they are not relevant to UI business functions.

Vulnerability Areas

Vulnerability results from a weakness in an agency's line of defense against threats, such as inadequate or non-existent controls (i.e., safeguards). These weaknesses provide the opportunity for loss to an asset or a set of assets when a threat occurs. RiskWatch provides 24 vulnerabilities; however, no vulnerability can be deselected in Phase I. RiskWatch provides the opportunity to select or deselect vulnerabilities in Phase III.

Safeguards

Safeguards are the technical, procedural, or environmental controls that protect an agency's assets from loss by eliminating or minimizing the vulnerabilities that lead to a realized threat. RiskWatch allows the user to select from 42 safeguard categories. Select those safeguard pertinent to the agency or business function. RiskWatch requires the user to select the safeguard by deselecting the inappropriate safeguards. New safeguards can be added. If safeguards are not deselected, RiskWatch includes all the safeguards in the case. The Project Team recommends combining or eliminating the following Safeguard Categories:

- Combine Classification Markings, Material Desegregation, and Security Classification into one category.
- Combine Security Plan, Security Policy, and Security Staff under Security Policy into one category.
- Combine Review of Sensitive Applications, Safeguard Test and Evaluations, and Risk Analysis into one category.
- Eliminate Technical Surveillance and Tempest Survey.

The term "combine" means to place all safeguards that fit into the referenced categories into the category indicated or the category most appropriate to the agency.

Phase II – Data

In Phase II, Data, RiskWatch requires the analyst to input data in four areas, or steps: Organization Parameters, Add/Edit Assets, Threat Frequencies, and Safeguard Details. Section 4, Ideas For Collecting and Organizing Data, provides details on where and how to find the data. The following provides an explanation of each area/step and the data elements associated with it.

Organization Parameters

This area defines the general properties of the agency or business function. RiskWatch uses the data elements with an asterisk (*) for calculations. The remaining data elements provide background information for reports.

- Name of Organization
- Number/Code of Organization Unit
- System to be analyzed
- How many days/week does the system operate? *
- How many hours/day does the system operate? *
- Down time before serious consequences
- Time to replace minimal functional support
- Data Sensitivity Level
- Security mode

- Number of full-time users
- For financial systems, Maximum dollars managed by the system
- Value of the mission for the enterprise, per annum *

Add/Edit Assets

In this step, the analyst inputs asset data. Each asset may require input for as many as six (6) data elements. Those data elements include:

- Replacement Cost for the asset
- Confidentiality Cost for the asset (usually a data set)
- Cost per hour of unavailability of the asset measured to include consequent unavailability of all other dependent assets
- A constant detection cost (or Auditing cost) for this asset
- Total Potential Cost to the Enterprise arising from this asset becoming contaminated. In general, this cost is in no way related to the basic costs of the asset
- Percentage of mission dependent on this asset

Threat Frequencies

In this step, the analyst inputs a Local Annual Frequency Estimate (LAFE) for each threat selected in Phase I. The LAFE represents the number of occurrences of a threat on an annual basis. As implied by the term "local", the LAFE reflects the particulars of a specific geographic area and the business function under analysis. RiskWatch also provides a Standard Annual Frequency Estimate (SAFE), which is also the LAFE default value. The SAFE is a national average.

Safeguard Details

Phase II's final step requires the analyst to provide data on the safeguards necessary to eliminate or minimize threats. On a category by category basis, the analyst inputs the following data:

- Implementation Cost
- Annual Maintenance Cost
- Percentage Implemented
- Lifetime (in years)

Question Phase

In the Question Phase, the analyst identifies the respondents, their Functional Areas, and selects the questions appropriate to the agency and the case. RiskWatch requires the analyst to perform six steps to complete the Question Phase.

Step 1. Edit/Select Questions

The analyst selects, edits, and modifies questions that RiskWatch provides with the template, as well as questions developed by other users (e.g., the UIRAP questions). This step eliminates questions not applicable to the agency, and modifies terminology to match that used and understood by perspective respondents in the agency's "local environment".

Step 2. Establish the Answer Threshold

Using the RiskWatch questionnaire program, respondents score the compliance levels of questions involving policy, procedure, security precautions, etc. The respondents use a scale of 0 to 100 percent. The analyst has responsibility, along with upper management, to establish an acceptable level of compliance for the business function under review. The RiskWatch default is 85 percent.

Step 3. Identify Respondents

In this step, the analyst determines which individuals have the knowledge and expertise necessary to accurately measure, or score, compliance. RiskWatch requires the analyst to input the respondent's name, to establish a respondent ID, and to select one or more Functional Areas appropriate to the respondent's position. RiskWatch then produces a set of questions packaged specifically for the respondent's designated Functional Areas.

Step 4. Prepare Question Sets

Preparing question sets allows the analyst to distribute questions to the respondent by disk, E-mail, LAN, etc. (See Memo to A Respondent.)

Step 5. Import Answers

Importing answers involves moving the respondents answers into the RiskWatch program by use of disk, e-mail, LAN, etc.

Step 6. Produce the Question Report

In this final step, RiskWatch assimilates the respondent's answers. Then individually or in multiple respondents, RiskWatch summarizes the answers to each question and produces the Vulnerability Report.

Phase III – Links/Executions

In Phase III, RiskWatch creates the links between the loss, asset, threat, and vulnerability categories. RiskWatch then uses the links, together with the input data, to calculate the Annual Loss Expectancy (ALE) and perform the Safeguard Evaluation.

Phase IV – Reports

RiskWatch produces a variety of reports that the analyst can tailor to meet the agency's needs. For details on the reports, refer to Section 4 RiskWatch Phase IV - Reports beginning on page 33.

Ideas For Collecting and Organizing Data

The section presents suggestions on where and what data the analyst can collect for use in completing each phase of RiskWatch, particularly Phase II, Data. First, this section lists general information the analyst might collect. This is followed by specific Phase by Phase suggestions for collecting and organizing the data, as well as suggested methods or steps for developing the figures needed by RiskWatch.

Collecting General Data

The Analyst should review the definition in the Appendix to select those categories appropriate to the agency or business function.

1. Interviews - Used to:
   - Identify business function tasks and workflow.
   - .Develop narratives, flow charts, etc.
2. Documentation
   - Logs – Use to determine threat annual frequency estimates (AFE) for the following:
     - System error rates, unauthorized access attempts, maintenance activities etc.
     - Facility maintenance problems such as electrical failure, heating/air-conditioning failures, elevators failures, security and fire suppression and detection, environmental control systems, etc.
     - Visitor's sign-in sheets to measure access control
   - Incident Reports

     Use to determine threat AFE, identify vulnerabilities, safeguards and questions to ask during the analysis for such threats as theft of assets or data, data destruction, security violation, internal fraud, data disclosure, data integrity loss, work place violence, false alarm, unauthorized building access, etc.
   - Standard Operating Procedure (S.O.P.) – Use as the control standard for (new) vulnerability questions.
3. Identify Safeguards (a.k.a. controls)
   - Existing Controls – Use to:
     - Describe current controls and their effectiveness.
     - Determine the safeguard's lifetime in years.
     - Determine the percentage the safeguard is implemented.
     - Determine implementation (i.e., initial or one-time) costs.
     - Determine maintenance (i.e., annual or ongoing) costs.

- Previous Audit Reports – Use to:
    - Identify previously reported threats and vulnerabilities.
    - Identify previously recommended safeguards.
    - Verify if recommendations were implemented and there effectiveness.
- Contingency Plans – Determine if:
    - Contingency plans exist for the business function.
    - The plan has been tested and/or the results documented.
    - The plan is kept current and distributed to the appropriate personnel.
    - Multiple copies are stored off site.
- Inventory Records – Use to:
    - Identify assets.
    - Determine asset replacement costs.
    - Determine asset life expectancy.

4. Facility Information – Use to identify assets, threats, and vulnerabilities. If available and appropriate, consider collecting:
    - Floor plans,
    - Address and location,
    - Structural information,
    - Lease agreements,
    - Security systems,
    - Insurance policies,
    - Fire systems, and
    - Plumbing, cabling, and electrical layout.
5. Personnel-Related Data – Use to:
    - Identify questionnaire respondents and their functional areas.
    - Identify separation of duty vulnerabilities.
    - Determine staff turnover rates.
    - Determine salary, benefit, training, and other personnel-related costs.
6. Mission Statements - Use as background material for reports.
7. System and Network Configurations – Use to identify assets (i.e., software, hardware, cabling), threats, and vulnerabilities.

8. Local Area Statistics
   Use to determine the Local Annual Frequency Expectancy (LAFE) for natural disasters. Sources to consider include State Emergency Management Agencies (SEMA), local fire and police departments, state statistics, etc.

From What Sources Is The Data Collected?

- Physical, System, and Internal Security
- Information Technology (IT)
- Program Specialists
- Users
- Facilities and Maintenance
- Financial Management
- Personnel
- Outside Sources (local fire and police, other agencies, SEMA, etc.)

Collecting Data for Input into RiskWatch

The following provides the type of data or the specific data elements that the analyst needs to collect for input into RiskWatch. The information is presented by the Phases used in RiskWatch.

RiskWatch Phase I – Selection

First, the analyst reviews the definitions in Appendix C and uses the data collected during preliminary research and from the above sources to select those categories appropriate to the organization or business function.

RiskWatch Question Phase

The complexity of the Question Phase warrants devoting a complete section to the step-by-step procedures. Refer to Section 6 for the Question Phase procedures.

RiskWatch Phase II - Data

Organization Parameters

RiskWatch uses 13 data elements to define the organization's parameters. The following lists those data elements and provides suggestions on how to determine what to put into them. RiskWatch uses the data elements with an asterisk (*) in its calculation; all other fields provide background data only.

1. Name of Organization
2. Number/Code of Organization Unit
3. System to be analyzed

4. How many days per week does the system operate? *
5. How many hours per day does the system operate? *
6. Downtime before serious consequences*
    - Determine how many hours the organization can go without the business function or system before serious consequences occur.
7. Time to replace minimal functional support*
    - Determine how many hours it takes the organization to resume minimal/essential operations for the business function or system or how soon basic operations are required to be up and running by state/agency requirements or expectations.
8. Data Sensitivity Level
    - Only four of the levels appear appropriate to the SESAs: Confidential, For Official Use Only, Not Applicable, or Privacy Act. Select the level most suitable to the business function or system's data.

TIP
Generally, for any risk analysis associated with UI, we suggest selecting "Privacy Act".

9. Security mode
    - RiskWatch provides six options: Dedicated, Limited Access, Multilevel, Not Applicable, Partitioned, and System High. RiskWatch provides no explanation of these options or the effect of their selection on the ALE or safeguard calculations, if any.

The Project Team advises using the Not Applicable option.

10. Number of full-time users*
    - Use the numbers of full-time employees (FTE) provided by the Agency's budget/fiscal office or count *any* employee who uses the system.
11. FOR FEDERAL SYSTEMS – Current Orange book level
    - Select Not Applicable, as this primarily applies to defense systems.
12. FOR FINANCIAL SYSTEMS – Maximum $ managed by the system
    - Use any of the following options, as appropriate to the business function:
        - The highest balance for the business function or system during the previous year
        - The highest allowable balance for the business function or system

13. Value of the MISSION for the enterprise, per annum.

> TIP
> The following suggestions do not represent all the possibilities for determining the value of the agency's mission.

- Use the method most suitable to the agency and business function.
- Document how Mission's value was determined.
- Use any of the following options:
  - A proportion of the agency's total budget for the business function.
  - The operating budget for the business function per year.
  - The outstanding collections due to the business function, such as BPC.
  - The trust fund balance.
  - A total or proportion the agency's accounts receivable balance.
  - The total taxes collected.
  - The total benefits paid out.

Add/Edit Assets

- Collecting For Input
  - Use pre-existing inventories and verify accuracy with business function experts.
  - Use a walk-through to collect and/or verify inventory data.
  - Use interviews to identify "unusual" inventory items, such as policies, procedures.

> TIPS
> Accuracy of inventory can be verified during a walk-through of the facility or business function.

  - Meet with the business function experts to identify all the assets necessary to conduct normal day-to-day operations.
  - Contact the fiscal office for asset data by cost center, expense code, and activity codes.
  - Establish "per person" or "per unit" costs for asset categories such as supplies and consumables, facility space (i.e., cost per square foot).

- Organizing For Input
  - Review the data collected prior to using RiskWatch to identify assets and missing data.
  - Use a worksheet for each asset, pulling the data from that previously collected. See Appendix A - Supplemental Data for a sample worksheet.
  - Organize asset data by workstation or employee, counting office-owned inventory separately.

As stated in Section 3, RiskWatch requires as many as six (6) data elements ($ or %) per asset depending on the asset category. Table 4 Asset Category Data Elements in Appendix A provides help to identify the assets and values required for RiskWatch. For each of the data elements, the guide provides, as appropriate, a translation of the data element terminology, UI related examples, and suggestions for where/how to develop the needed values. The requested values include:

1. Replacement Cost for the Asset (Direct Loss).

   In addition to the items that RiskWatch suggests in its definition of asset categories, consider including the items in the UI Related provided in Appendix A-Supplemental Data for Table 5 Replacement Cost. However, neither the RiskWatch's definitions nor the UI Related Examples, are all inclusive.

2. Confidentiality cost for the asset (usually a data set) (Disclosure)

TRANSLATION
The cost associated from disclosure of confidential information can prove to be greater than the replacement cost value. The higher value relates to future loss projections associated from bad publicity that an agency can receive from the fallout of the data disclosure.

EXAMPLE
Unauthorized disclosure of data includes wage, claim, and/or employer data. Awards of $1,000 to $5,000 per individual record have been assessed by the courts based on the sanctions included in the Privacy Act of 1974.

TIP
Sensitivity level is important especially with data protected by the Privacy Act of 1974. The Privacy Act is very specific on the scope and requirements for data protection.

Refer to Appendix A-Supplemental Data, Table 6 Confidentiality Cost for the Asset (Disclosure), for UI related examples and suggestions on developing Confidentiality Cost.

3. Cost per hour of unavailability of the Asset measured to include consequent unavailability of all other dependent assets (Delay/Denial).

TRANSLATION
The cost resulting from a delay or denial of service or productivity due to a realized threat to an asset. This cost includes the cost of downstream assets that also become unavailable.

- Determine the length of time that service can be unavailable without resulting in an unacceptable effect on the business function. The hours from the "Down time before serious consequences" from the Organization Parameters can also be used.
- When determining the cost per hour, identify the secondary (i.e., dependent) assets that become unavailable when the primary asset is unavailable.
- There are two types of labor costs: operational and make-up.
  - Operational cost relates to the labor associated with ongoing, normal production that is lost when the asset becomes unavailable.
  - Make-up cost is the labor for processing backlogs or resuming normal operations after an asset is recovered, replaced, etc.

EXAMPLE
<u>Operational cost</u>
500 (users) x $15 (average hourly wages) = $7,500 loss per hour
$7,500 (loss/hour) x 8 (hours downtime) = $60,000 total loss

<u>Make-up cost</u>
$15 (average hourly wage) x 150% (overtime rate) = $22.50 per hour
500 (users) x $22.50 (average OT rate) = $11,250 loss per hour
$11,250 (loss per hour) x 4 (hours to process backlog) = $45,000

Appendix A, Table 7 Cost Per Hour of Unavailability of the Asset (Delay/Denial) provides specific UI related examples and suggested values or items for inclusion in the delay/denial cost for each asset category listed.

4. A Constant Detection (or Auditing) Cost for the Asset (Modification)

TRANSLATION
The cost associated with protecting the asset from unauthorized or unintentional modification. Examples include: virus detection software, reviewing system logs, installing proxy servers or firewalls to detect unauthorized access attempts, conducting user reviews, conducting tax audits or quality control, internal security, or employer and claimant fraud detection activities.

EXAMPLE
A firewall keeps hackers from attacking the system. Without the firewall, the system could be modified. This cost includes the firewall's purchase price and the hourly staff to monitor the system.

RiskWatch requires this data for the following asset categories:

- Accounts Payable
- Accounts Receivable
- Applications
- Cash Accounts
- Communications Software
- Data Bases
- Negotiable Instruments
- System Software

5. Total Potential Cost to the Enterprise arising from the Asset becoming contaminated. In general, this cost is in no ways related to the basic cost of the Asset. (Modification)

Generally, cost increases proportionately with the degree to which internal controls are implemented and effective in reducing or eliminating the likelihood and scope of asset contamination. Operating on this premise, the Project Team suggests using a percentage of the total asset's value (i.e., replacement cost) as the cost of contamination. The percentage is based on the level of **ALL** controls (i.e., safeguard) currently in place to protect the asset. The Project Team has provided the following scales for consideration:

- Strong controls: 1%
  100%-implemented controls have proven themselves highly effective through the substantial reduction, elimination, or non-existence of asset contamination.
- Moderate to strong controls: 5%
  75% - 99% implemented controls have proven themselves generally effective through the reduction of asset contamination.
- Weak to moderate controls: 10%
  25% - 74% implemented controls marginally effective in reducing asset contamination.
- Non-existent to weak controls: 20%
  0% - 24%-implemented controls have proven of little to no value in reducing asset contamination.

EXAMPLE
The Total Potential Cost to the Enterprise arising from the UI database becoming contaminated is based on the Replacement Cost value of $25,000 because the organization performs regular back-ups of the database (refer to Table 5 Replacement Cost). However, the overall controls (i.e. Safeguards) not fully implemented to the production database are only 45%. This places the asset's internal controls in the weak to moderate category. Calculating the contamination cost at 10% of the asset's Replacement Cost ($25,000), the loss equals $2,500.

RiskWatch requires this data for the following asset categories:

- Accounts Payable
- Accounts Receivable
- Applications
- Cash Accounts
- Communications Software
- Data Bases

- Negotiable Instruments
- System Software

6. Percentage of Mission dependent on this Asset (Related Direct Loss).

TRANSLATION
This equals the percentage of the business function that relies on the asset. (The "mission" is for the business function under analysis.)

EXAMPLE
If the mainframe became unavailable, what percentage of the day-to-day operations for the business functions would cease? If day-to-day operation could only operate at 25% capacity, then 75% of the mission is dependent on this asset.

TIP
RiskWatch will not allow the analyst to use a percentage less than 5%.

RiskWatch requires this data for the following asset categories:

- Accounts Payable
- Accounts Receivable
- Applications
- Communications Hardware
- Communications Software
- Data Bases
- Facilities
- Hardware
- Intangibles
- Personnel
- Support Systems
- System Software

Threat Frequency

RiskWatch software provides two measurements of threat frequency:

- **SAFE - "Standard Annual Frequency Estimate"**
- **LAFE - "Local Annual Frequency Estimate"**

The SAFE represents a fixed national average that the user cannot modify. However, in Phase II, LAFE can and should be adjusted to match the conditions in the geographical area and for the business function. RiskWatch uses the LAFE figures to calculate the Annual Loss Expectancy. If unsure of or unable to determine a LAFE appropriate for the case, use the standard (SAFE) provided by RiskWatch. The table below provides a guide on how to convert frequency estimates for use in RiskWatch.

Table 1 Annual Frequency Estimate

Once a year	1	Once every 2 years	.5
Twice a year	2	Once every 5 years	.2
Five times a year	5	Once every 10 years	.1
Ten times a year	10	Once every 20 years	.05
Fifty times a year	50	Once every 50 years	.02
Hundred times a year	100	Once every 100 years	.01

If data is missing, try the suggested sources in the table below. If data is unavailable, request that the appropriate business function expert to provide a reasonable/best judgement estimate, or use the analyst's best judgement. For suggested sources for threat LAFE, refer to Table 8 Local Annual Frequency Sources in Appendix A.

Safeguard Details

- RiskWatch has four fields that require data entry:
  - Implementation Cost
  - Annual Maintenance Cost
  - Percentage Implemented
  - Lifetime (in years)
- To develop the necessary safeguard data, The Project Team suggests following the steps outlined below:
  1. Review the list of Safeguards to verify if appropriate for the review. If changes are necessary, return to Phase I, Selection, to select/deselect categories.
  2. Include all existing safeguards for the business function.
  3. Identify necessary safeguards not implemented from the question response report (vulnerability report).

EXAMPLE
Existing contingency planning safeguards 100% are implemented, but in the analysis, back-up power is discovered lacking. Redundant power is chosen as the safeguard, but indicate 0% implemented.

TIP
A safeguard is needed for any vulnerability question with an average response below your threshold (See Question Phase for definition).

  4. Determine into which safeguard category each specific safeguard fits.
  5. Total the cost of all the safeguards for each category.
  6. Select the safeguards to be recommended to management based on their ability to reduce the vulnerabilities.
- Suggested sources for implementation and maintenance cost, percent implemented, and lifetime figures include:
  - Information Technology
  - Business function manager
  - Fiscal Management
  - Vendors
  - Other state agencies

  - Security officers (i.e. Internal, Physical, and Information)
  - Audit reports
  - Internet
- The following lists methods and sources for each of the safeguard data elements.
  - To determine safeguard Implementation Cost, use one of three options:
    - Full implementation cost (See Asset Replacement Cost Table).
    - Actual cost incurred to complete 100 % safeguard implementation.
    - Use specified period (i.e. actual implementation cost over a two-year period for existing safeguards).

> TIP
> Whichever option the analyst chooses be consistent throughout the analysis.

  - To determine the Annual Maintenance Cost consider one or more of following:
    - Upgrade fees
    - Labor cost
    - Vendor/contract cost
    - Data center cost
    - Usage fees
    - Other costs that are determined appropriate
  - To determine the safeguard's Lifetime, use:
    - Vendor supplied data
    - Historical records
    - Use RiskWatch defaults
  - To determine the percentage implemented:
    - Request Information from management
    - Feedback from program experts

> TIP
> For multiple safeguards within a category, use the average percentage implemented.

- To determine the reduction for this safeguard in:
  - Asset Values
  - Threat Frequency
  - Effective Level of Vulnerability

Warning:
Due to the complexity and level of effort required to change these percentages, it is ***strongly*** recommended that the RiskWatch default values be used.

RiskWatch Phase III – Relationship and Program Execution

Phase III establishes the relationships between losses, assets, threats, and vulnerabilities to arrive at tangible loss estimates. This phase has three activities: linking relationships, Annual Loss Expectancy (ALE) calculation, and safeguard evaluation. The user establishes and verifies the relationships and RiskWatch automatically performs the ALE calculation and safeguard evaluation.

Linking Relationships

In a series of three steps, RiskWatch defines the relationships between the assets, losses, threats, and vulnerabilities. In all three steps, the only action required of the user is to review the relationships between them. However, in Step 3:, RiskWatch provides the option of using the default relationships or adding/deleting/changing relationships.

Step 1: Asset/Loss Incidents:
RiskWatch defines the relationship between the asset and loss categories. RiskWatch refers to this combination as an *incident class.*

Step 2: Asset/Threat/Loss Incidents:
RiskWatch defines the relationship between the incident class and the threats; with a threat potentially having multiple incident classes. RiskWatch refers to this asset-loss-threat relationship as an *incident*.

Step 3: Asset/Threat/Loss/Vulnerability Links:
Determination of Annual Loss Expectancy (ALE): Product of Impact ($ Value) and Frequency of Occurrence (once a year)

WARNING
If the RiskWatch defaults are changed in this Phase, **THE ANALYST** is at risk of having to reenter all data from the beginning. It is advised to ONLY review the defaults setting to become familiar with the Links/Relationships.

Step 1:Asset/Loss Incident Classes

RiskWatch previously set the links. This is an area for review purposes and no changes should be needed.

Step 2:Asset/Threat/Loss Incidents

RiskWatch reviews the threat and loss category for each asset within the designated asset category and review the asset(s) linked. There would be a loss to that asset if that threat occurred. RiskWatch assigns each incident (loss-asset-threat combination) a Degree of Seriousness (SE).

TIP
More experienced users may want to evaluate the SE in terms of its effects on the business function analysis. See Appendix A Form 7 for RiskWatch's default SE values for each incident.

Degree of Seriousness (SE)

In Step 2 above, RiskWatch assigns each incident a Degree of Seriousness (SE). The SE is expressed in two forms: hours or percentages. For the Delay/Denial Loss Category, the SE is measured in hours. The hours represent the length of time that the asset is unavailable. For all remaining loss categories, Direct Loss, Disclosure, Intangibles, Modification and Related Direct Loss, the SE is stated as a percentage of the asset lost. In either case, the greater the SE, the larger the loss.

EXAMPLE
Delay/Denial Category SE: 8.0 represent 8 hours that the asset is unavailable due to a realized threat.

All other Loss Categories: 1.0 equals 100% loss of asset; 0.1000 equals a 10%; .0100 equals 1%; .0010 equals 1/10th of 1% loss; and .0001 equals 1/100th of 1% loss.

RiskWatch uses the SE to calculate the Single Loss Expectancy (SLE). The SLE equals the loss resulting from a single (or one-time) occurrence of a threat. RiskWatch uses the following formulas to calculate the SE for the corresponding Loss Category:

Table 2 Calculating the Degree Of Seriousness

Loss Category	Formula	Translation
Direct Loss	Se*RCa	SE x Replacement
Disclosure	Se*Cca	SE x Confidentiality Cost
Delay/Denial	Se*UACa	SE x Cost per hour of unavailability of the asset measured to include consequent unavailability of all other dependent assets.
Modification	DeC+(Se (RCAa+Pca))	A constant detection cost for this asset + (SE x (Replacement Cost + Total Potential Cost to the Enterprise arising from this asset becoming contaminated.))
Related Direct Loss	Se*PMD	SE x Percentage of mission dependent on this asset.

Step 3:Asset/Threat/Loss/Vulnerability

RiskWatch previously set links. This is an area for review purposes and no changes may be needed.

ALE Calculation

The only requirement of the analyst is to select the ALE calculation box. (The ALE is the Annual Loss Expectancy.) RiskWatch automatically calculates the ALE using the following formula: SLE x LAFE = ALE. RiskWatch uses the above SLE formulas together with the LAFE input by the analyst to arrive at the ALE.

WARNING
RiskWatch may display a **Warning: Missing Incident Data** dialog box. Print this report and review the information to determine what, if any, changes are needed to the data.

Single Loss Expectancy

If the marriage between these elements were to occur one time, the loss would be considered a single loss expectancy (SLE). To determine the loss on an annual basis, the SLE is multiplied by the threats annual frequency of occurrence. SLE multiplied by the annual frequency = annual loss expectancy (ALE).

Safeguard Evaluation

The only requirement of the analyst is to select the Safeguard Evaluation box. RiskWatch automatically performs this evaluation.

What Ifs

What IF reports are optional. RiskWatch provides two What IF reports: Safeguards vs. Threats and Threats vs. Safeguards. The Safeguards vs. Threats report lists all threats that will impact a selected safeguard. It also provides the ALE with and without implementation of the safeguard. Similarly, the Threats vs. Safeguard report lists all safeguards that impact the selected threat and, again, provides the ALE with and without the implemented safeguard.

RiskWatch Phase IV - Reports

Phase IV concludes the risk analysis process with a set of reports from which the user selects. The user can omit or edit the reports. Below is a description of each report's contents and suggestions on how to tailor the report to the agency's or business function's needs.

Introduction, Executive Summary, and Recommendations

RiskWatch uses standard templates for the Introduction, Executive Summary, and Recommendations that fail to amend themselves according to the input data. This requires the analyst to completely rewrite these sections.

Asset Reports

RiskWatch produces two asset reports: A Summary by Asset Report and a Full Asset Report. The summary by Asset reports lists the asset categories in descending order by total asset value. The Full Asset report list the individual assets included in each asset category. The Full Asset Report also displays various bar and pie charts that graphically illustrate an individual asset's value in proportion to the value of the whole asset category.

Threat Reports

RiskWatch produces two threat reports: A Summary by Threats Report and a Full Threat Report. The Summary by Threats Reports lists the threat categories in descending order by total loss value. The Full Threat report lists, by threat, the AFE, incident calls associated with the threat, the SLEs and ALEs per incident class, and the percentage of the total ALE that the incident class' ALE represents.

Vulnerability Reports

RiskWatch produces two reports based on the question responses: A Vulnerability Distribution Report and Full Vulnerability Report. The Vulnerability Distribution Report lists the 50 question with the lowest individual responses and their corresponding vulnerability area. Some questions can be identified more than once. However, the Project Team could not determine if the report presented the questions in a specific order or randomly. The report concludes with a table indicating the number of question appearing in each vulnerability area and a corresponding pie chart that displays the same information using percentages.

The Full Vulnerability Report indicates for each vulnerability area the percentage of compliance and non-compliance. RiskWatch provides no explanation of how it calculates the percentages.

Safeguard Reports

RiskWatch produces three cost-benefit analysis reports: A Safeguard-Threat Report, a Full Safeguard Report, and a Cost-Benefit Report. The Safeguard-Threat Report lists the threats addressed by each safeguard category, along with the Original ALE, the

ALE with Safeguard (i.e., the reduced ALE after safeguard implementation), and the Percentage Drop (in ALE). The report concludes with a bar chart displaying the difference in descending order.

The Full Safeguard Report provides a cost benefit analysis by safeguard category. It calculates the year-by-year benefits and costs for the safeguard's expected lifetime, as well as calculations by discount factors of 5, 10, and 15 percent. However, RiskWatch provides no explanation of how it produces its figures. Listed below is the information included in this report and the Project Team's explanation of the calculations as determined through analysis. The User's Guide only explains the 10 percent discount rate.

Year-by-year calculations based on the safeguard's estimated lifetime.

- Benefits: This appears to equal the difference between the Original ALE and the ALE with Safeguard from the Safeguard-Threat Report.
- Costs: For the first year this equals the one-time cost; for subsequent years, it equals the maintenance costs.
- Discounted Benefits: This equals the Benefits multiplied by a yearly discount factor. The discount factors match those found in the Department of Labor's 1987 Technical Assistance Guide:
  - Year 1 - .909
  - Year 2 - .826
  - Year 3 - .751
  - Year 4 - .683
  - Year 5 - .621
- Discounted Costs: Calculated the same as Discounted Benefits.
- Discounted Benefits minus Discounted Costs: Self-explanatory.
- Calculations by discount factors
  - Sum of Discounted Benefits: Equals the sum of each year's Discounted Benefits.
  - Sum of Discounted Costs: Equals the sum of each year's Discounted Costs.
  - Benefit Cost Ratio: Equals the Sum of Discounted Benefits divided by the Sum of Discounted Costs.
  - Return on Investment: Appears to equal the Discounted Benefits divided by the Sum of Discounted Costs.
  - Payback Period (in years): Appears to equal the Discounted Benefits minus Discounted Costs divided by the first year's Discounted Costs.

A summary of each safeguard's Return of Investment concludes this report.

Cost Benefit

The Cost-Benefit Analysis report analyzes the expected annual ALE reduction using the benefits and costs (implementation and maintenance) over the safeguard's lifetime. The analysis also considers three different possible discount rates of 5, 10, and 15 percent to permit the calculation of the net present value of all projected figures. For each safeguard, RiskWatch provides the following information for all three discount rates:

- The ratio of Total Benefits over Total Costs;
- The annualized Rate of Return on Investment obtained by dividing the above ratio by the number of years involved;
- The Payback Period – the year in which accumulated benefits overtake the (initially greater) accumulating costs.

This page left blank intentionally.

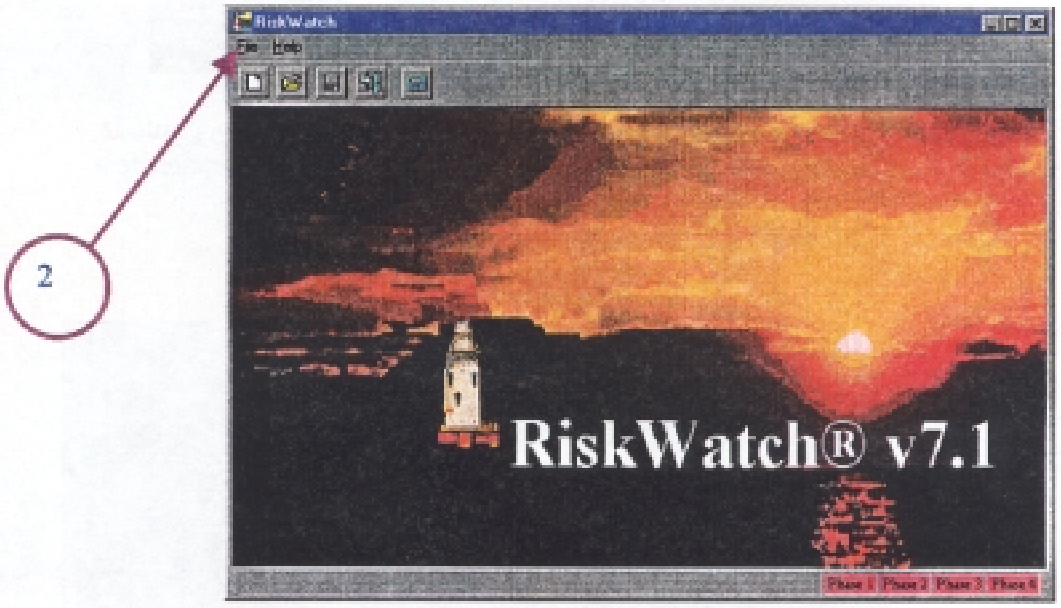
Using RiskWatch A Step-By-Step Approach

This section provides the analyst with the basic step-by-step instructions on how to use RiskWatch. It takes the analyst through a series of tasks, such as Creating a Case, selecting categories or inputting data, and provides explicit instruction on how to complete the task. Whenever possible, RiskWatch screen prints are provided. The circled numbers with arrows correspond to the step number for the task addressed. All the instructions relate to a test case.

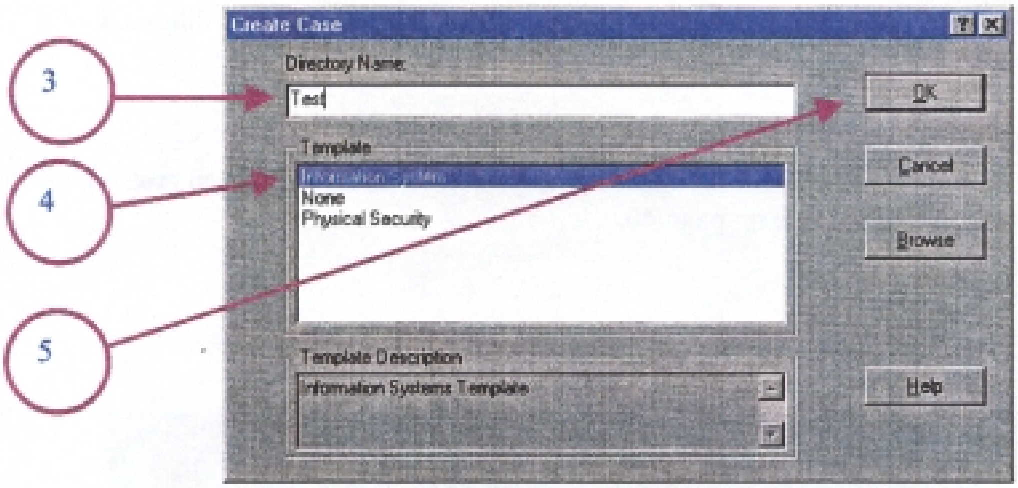
Creating A Case

If case was not previously created, follow the steps below. If case has been created, go to Opening An Existing Case on page 40.

1. Open RiskWatch.
2. Select **File, New**. The Create Case dialog box will appear.



3. For this guide, the case name will be "Test". Enter the name of your case.
4. Highlight the **Information System** template. (Note: This is the only template available on RiskWatch Basic 7.1.)
5. Select **O.K.**

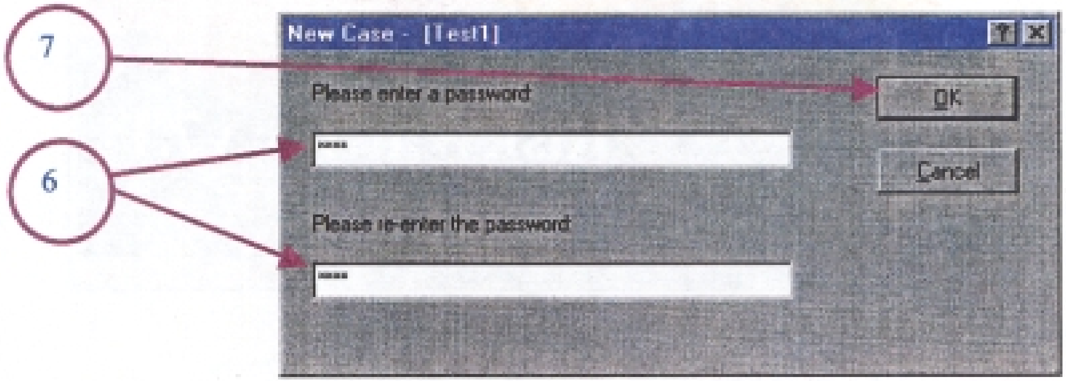


Directory Name: Test

Template: Information System (highlighted)
None
Physical Security

Template Description: Information Systems Template

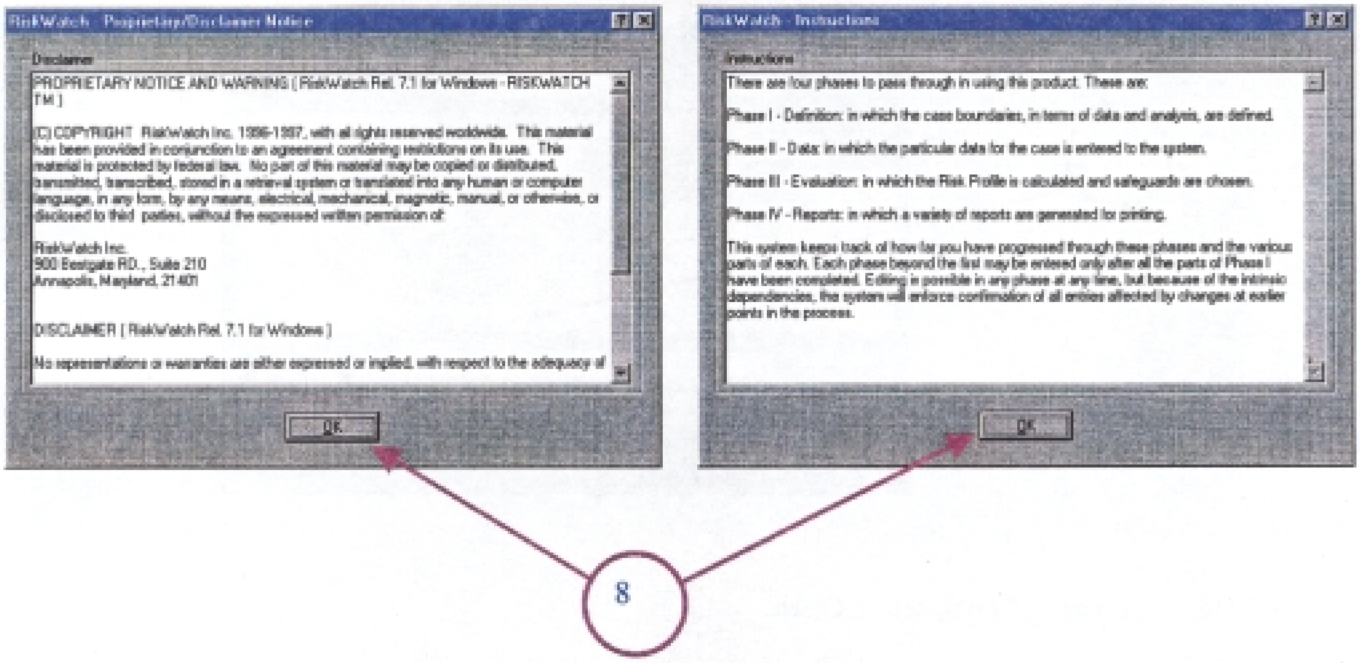
6. RiskWatch needs a password for the case. The password used for this guide is "test". Enter your password. Tab to "Please re-enter the password" Reenter test again.
7. Select **O.K.**



Please enter a password: ****

Please re-enter the password: ****

8. RiskWatch then requests that the analyst read the Disclaimer Notice and Instructions. After reading each, Select **O.K.** If the analyst chooses to quit at this point, save the case.



PROPRIETARY NOTICE AND WARNING [RiskWatch Rel. 7.1 for Windows - RISKWATCH TM]

(C) COPYRIGHT RiskWatch Inc. 1996-1997, with all rights reserved worldwide. This material has been provided in conjunction to an agreement containing restrictions on its use. This material is protected by federal law. No part of this material may be copied or distributed, transmitted, transcribed, stored in a retrieval system or translated into any human or computer language, in any form, by any means, electrical, mechanical, magnetic, manual, or otherwise, or disclosed to third parties, without the expressed written permission of:

RiskWatch Inc.
900 Eastgate RD., Suite 210
Annapolis, Maryland, 21401

DISCLAIMER [RiskWatch Rel. 7.1 for Windows]

No representations or warranties are either expressed or implied, with respect to the adequacy of

There are four phases to pass through in using this product. These are:

Phase I - Definition: in which the case boundaries, in terms of data and analysis, are defined.

Phase II - Data: in which the particular data for the case is entered to the system.

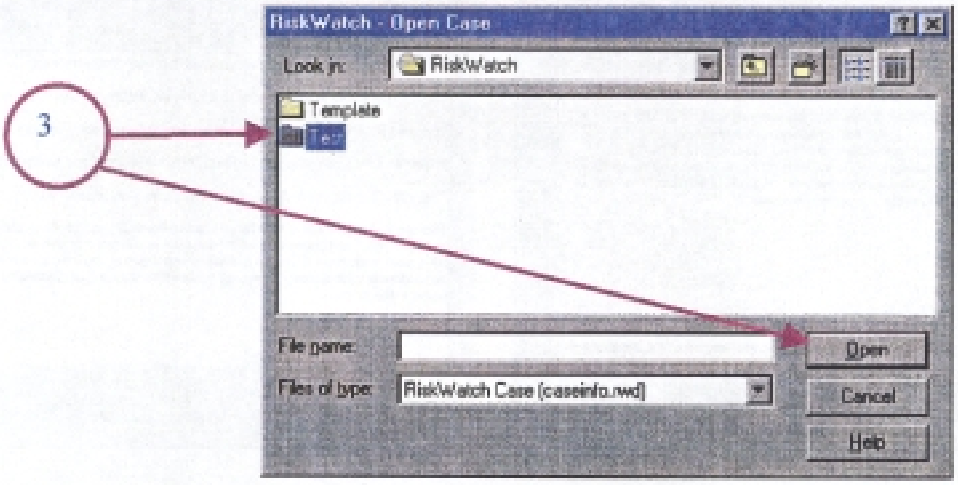
Phase III - Evaluation: in which the Risk Profile is calculated and safeguards are chosen.

Phase IV - Reports: in which a variety of reports are generated for printing.

This system keeps track of how far you have progressed through these phases and the various parts of each. Each phase beyond the first may be entered only after all the parts of Phase I have been completed. Editing in possible in any phase at any time, but because of the intrinsic dependencies, the system will enforce confirmation of all entries affected by changes at earlier points in the process.

Opening An Existing Case

1. Open RiskWatch.
2. Select **File, Open.**
3. Highlight the review Case Folder and Select **Open**.



RiskWatch - Open Case

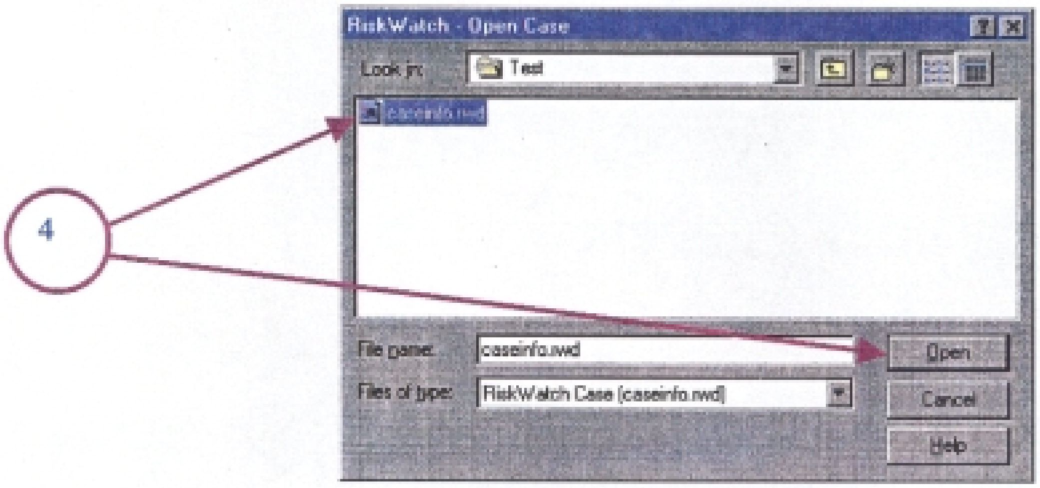
Look in: RiskWatch

Template
Test

File name:

Files of type: RiskWatch Case (caseinfo.rwd)

4. Highlight **caseinf.rwd**, select **Open**.



RiskWatch - Open Case

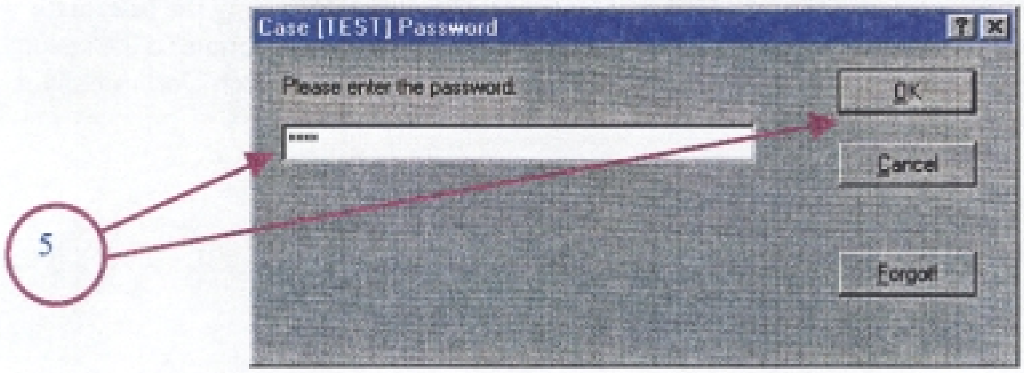
Look in: Test

caseinfo.rwd

File name: caseinfo.rwd

Files of type: RiskWatch Case (caseinfo.rwd)

5. **Enter** password for review case, Select **O.K.** The Overview dialog box appears. Data entry for all Phases of case can now be completed for the business function.


Case [TEST] Password

Please enter the password.

****

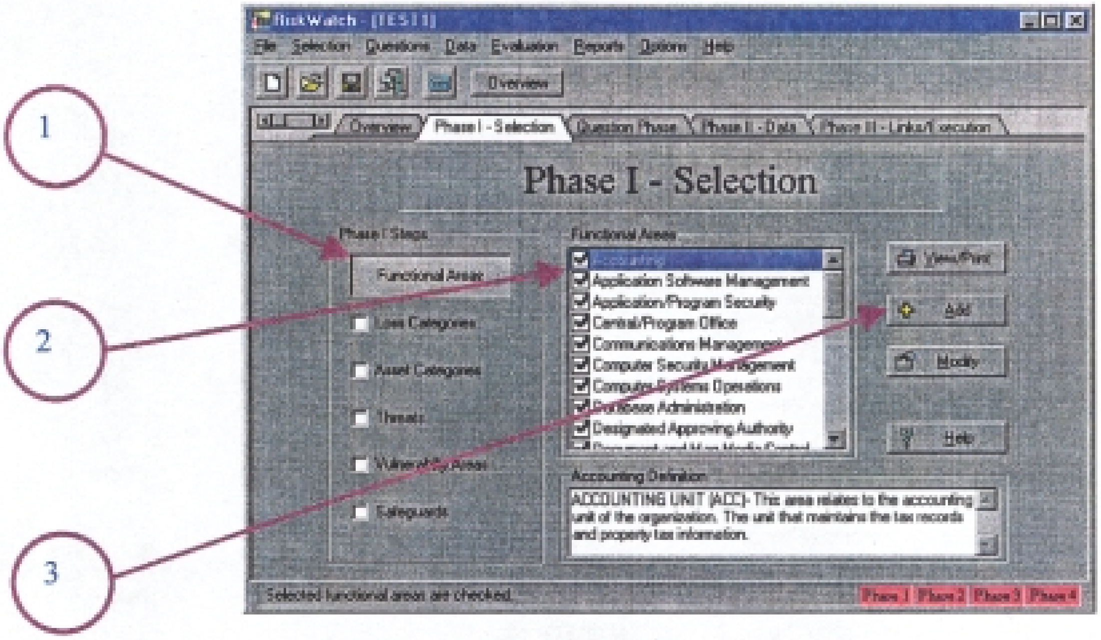
6. If referred here from any section, return to that section now.

Phase I - Selection

RiskWatch's default settings include all categories in each of the six areas: Functional Areas, Loss, Assets, Threats, Vulnerabilities, and Safeguards. Using the information gathered in Section 4, the analyst deselects the categories inappropriate to the agency of business function for each area. Refer to Appendix C, RiskWatch Definitions for the category definitions.

Functional Areas

1. Click **Functional Areas** in the Phase I tab.
2. **Click** on check mark in box to deselect Functional Areas.



Functional Areas

- ☑ Accounting
- ☑ Application Software Management
- ☑ Application/Program Security
- ☑ Central/Program Office
- ☑ Communications Management
- ☑ Computer Security Management
- ☑ Computer Systems Operations
- ☑ Database Administration
- ☑ Designated Approving Authority

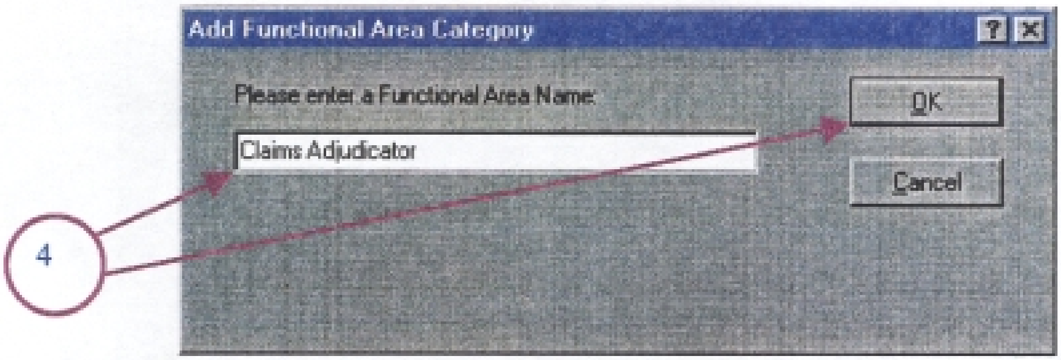
Accounting Definition

ACCOUNTING UNIT (ACC)- This area relates to the accounting unit of the organization. The unit that maintains the tax records and property tax information.

Selected functional areas are checked.

Adding a Functional Area

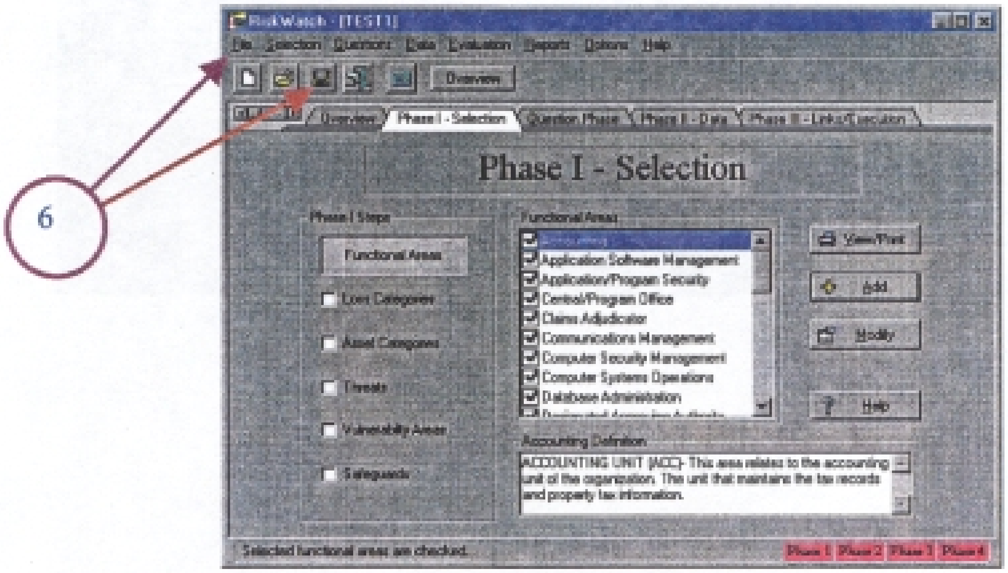
3. Select **Add** (see graphic on previous page). The dialog box Add Functional Area Category appears.
4. **Enter** the name of new Functional Area, and select **O.K.** A definition cannot enter.



Please enter a Functional Area Name: Claims Adjudicator

TIP
When adding new a Functional Area document the definition in the work papers.

5. Repeat step 4 for each additional new Functional Area.
6. **File, Save** or use the Save **icon.**



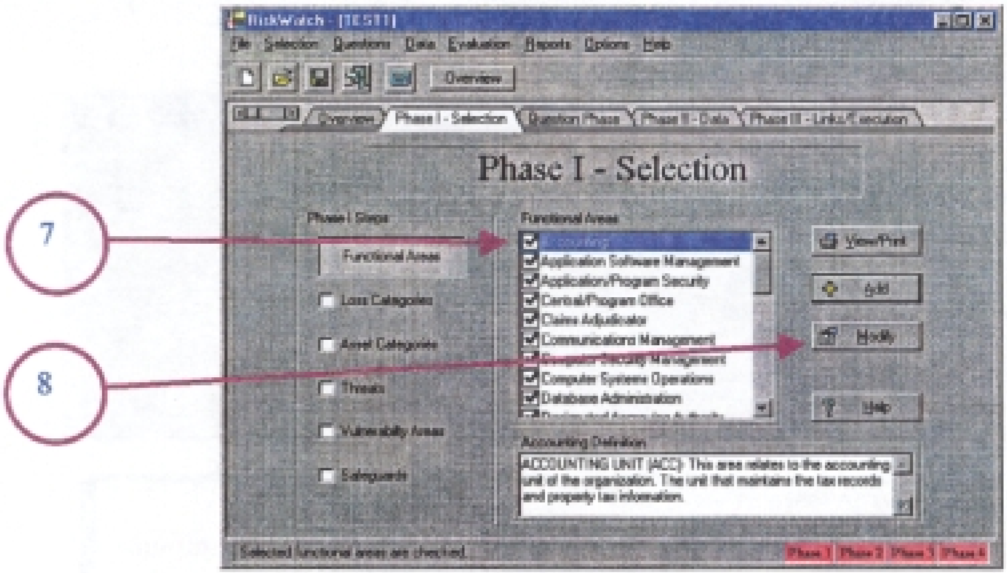
Functional Areas:
- ☑ Accounting
- ☑ Application Software Management
- ☑ Application/Program Security
- ☑ Central/Program Office
- ☑ Claims Adjudicator
- ☑ Communications Management
- ☑ Computer Security Management
- ☑ Computer Systems Operations
- ☑ Database Administration

Accounting Definition: ACCOUNTING UNIT (ACC)- This area relates to the accounting unit of the organization. The unit that maintains the tax records and property tax information.

Selected functional areas are checked.

Modify a Functional Area

7. Highlight the functional area that needs modifying.
8. Select **Modify**. The dialog box Modify Functional Area Category appears.

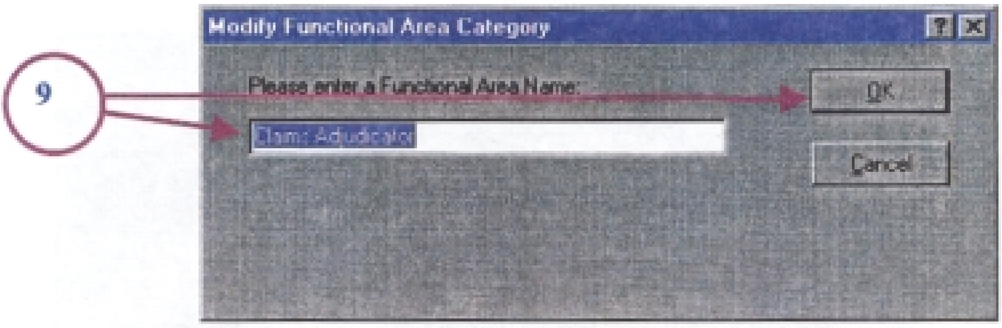


☑ Accounting
☑ Application Software Management
☑ Application/Program Security
☑ Central/Program Office
☑ Claims Adjudicator
☑ Communications Management
☑ Computer Security Management
☑ Computer Systems Operations
☑ Database Administration

ACCOUNTING UNIT (ACC): This area relates to the accounting unit of the organization. The unit that maintains the tax records and property tax information.

Selected functional areas are checked.

9. Enter the revised name of the Functional Area, and select **O.K.** A new definition cannot be entered nor does RiskWatch carryover the old definition.



Please enter a Functional Area Name:

Claims Adjudicator

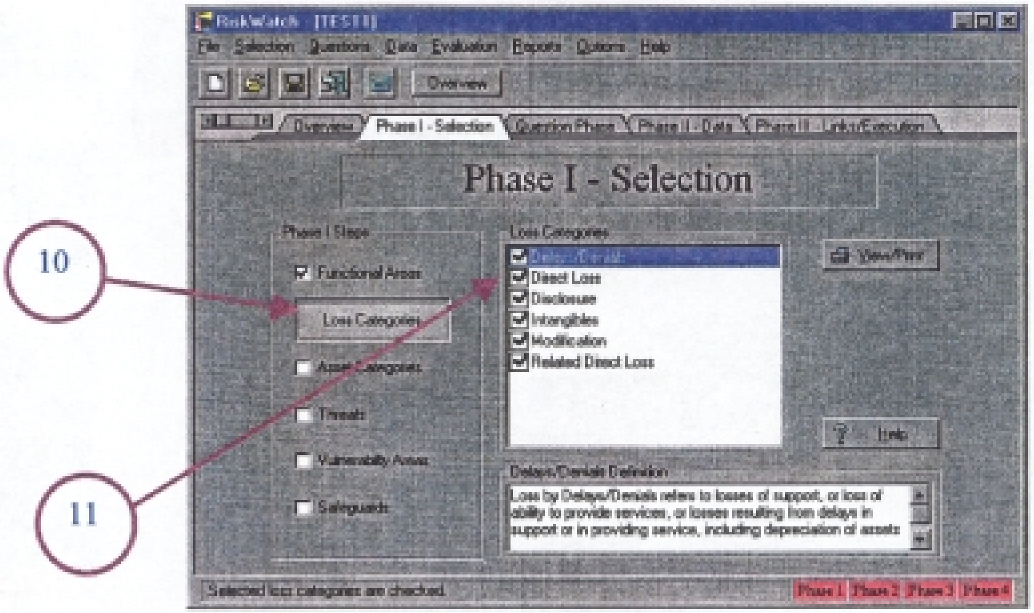
TIPS
Document reasons for deselecting a Loss Category or any category from Assets, Threats, Vulnerability Areas, or Safeguards.
If an asset needs to be reselected or deselected in a later Phase, the analyst can return to Phase I at any time.

Loss Categories

10. Click **Loss Categories** in the Phase I – Selection Tab.

11. **Click** on check mark in box to deselect a Loss Category.

TIP
Use all six categories, especially if a first time user.
Document reasons for deselecting a loss category.



Phase I Steps
☑ Functional Areas
Loss Categories
☐ Asset Categories
☐ Threats
☐ Vulnerability Areas
☐ Safeguards

Loss Categories
☑ Delays/Denials
☑ Direct Loss
☑ Disclosure
☑ Intangibles
☑ Modification
☑ Related Direct Loss

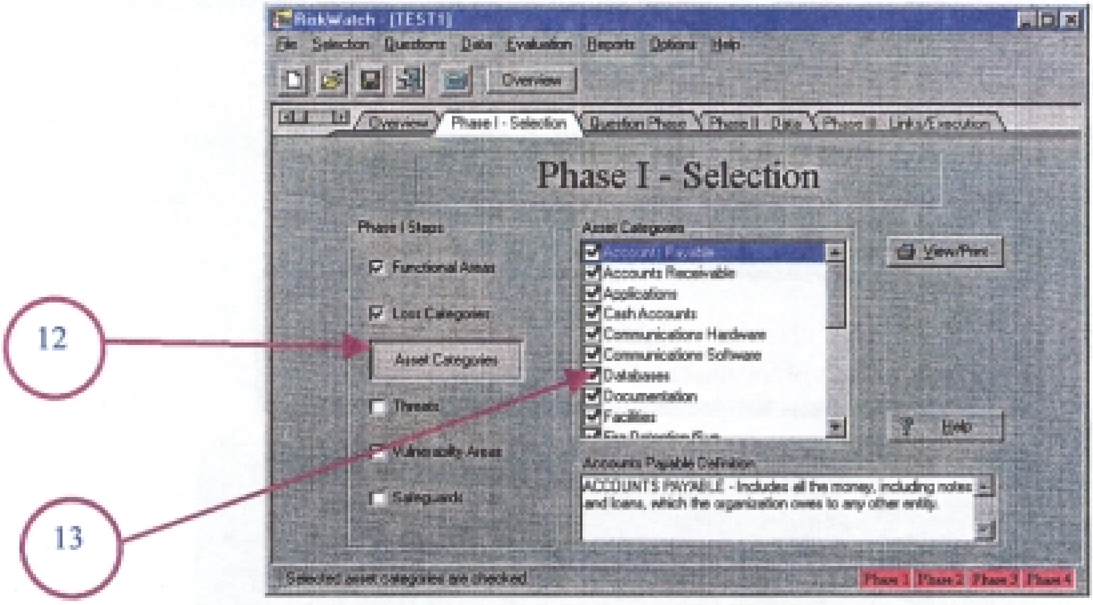
Delays/Denials Definition
Loss by Delays/Denials refers to losses of support, or loss of ability to provide services, or losses resulting from delays in support or in providing service, including depreciation of assets

Selected loss categories are checked.

Asset Categories

12. **Click** Assets Categories in the Phase I – Selection Tab.

13. **Click** on check mark in box for each Asset Category to deselect.



Phase I Steps

- ☑ Functional Areas
- ☑ Loss Categories
- Asset Categories
- ☐ Threats
- ☐ Vulnerability Areas
- ☐ Safeguards

Asset Categories

- ☑ Accounts Payable
- ☑ Accounts Receivable
- ☑ Applications
- ☑ Cash Accounts
- ☑ Communications Hardware
- ☑ Communications Software
- ☑ Databases
- ☑ Documentation
- ☑ Facilities
- ☑ Fire Detection Sys...

Accounts Payable Definition

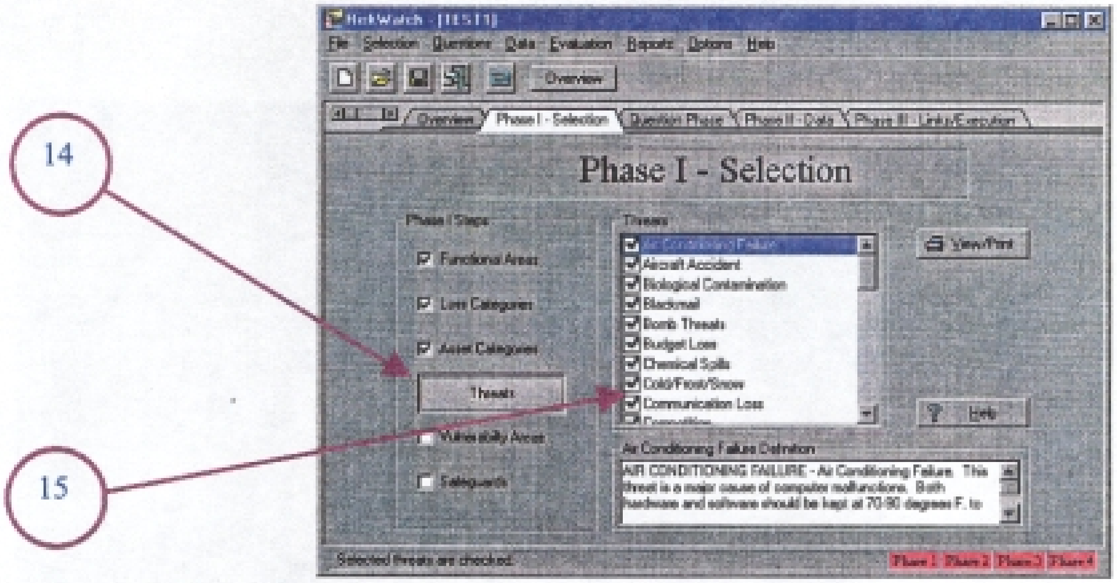
ACCOUNTS PAYABLE - Includes all the money, including notes and loans, which the organization owes to any other entity.

Selected asset categories are checked

Threats

14. Click **Threats** in the Phase I – Selection Tab

15. **Click** on check mark in box to deselect a Threat.



☑ Functional Areas
☑ Loss Categories
☑ Asset Categories
Threats
☐ Vulnerability Areas
☐ Safeguards

☑ Air Conditioning Failure
☑ Aircraft Accident
☑ Biological Contamination
☑ Blackmail
☑ Bomb Threats
☑ Budget Loss
☑ Chemical Spills
☑ Cold/Frost/Snow
☑ Communication Loss

Air Conditioning Failure Definition

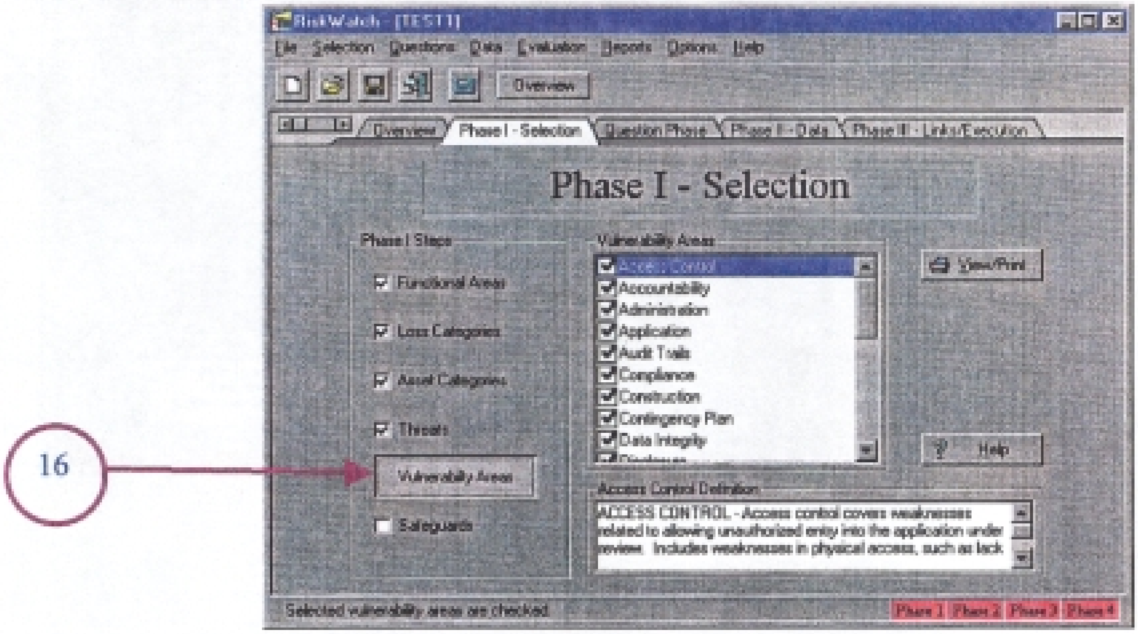
AIR CONDITIONING FAILURE - Air Conditioning Failure. This threat is a major cause of computer malfunctions. Both hardware and software should be kept at 70-80 degrees F. to

Selected threats are checked.

> TIP
> Annual Frequency Estimates will be entered in Changing Threat Frequencies.

Vulnerability Areas

16. Click **Vulnerability Areas** in the Phase I – Selection Tab. RiskWatch's default settings include all Vulnerability Areas; however, they cannot be deselected in Phase I. RiskWatch provides the opportunity to select or deselect vulnerabilities in Phase III - Relationships and Program Execution.



Phase I Steps

☑ Functional Areas

☑ Loss Categories

☑ Asset Categories

☑ Threats

☐ Safeguards

Vulnerability Areas

☑ Access Control
☑ Accountability
☑ Administration
☑ Application
☑ Audit Trails
☑ Compliance
☑ Construction
☑ Contingency Plan
☑ Data Integrity
☑ Disclosure

Access Control Definition

ACCESS CONTROL - Access control covers weaknesses related to allowing unauthorized entry into the application under review. Includes weaknesses in physical access, such as lack

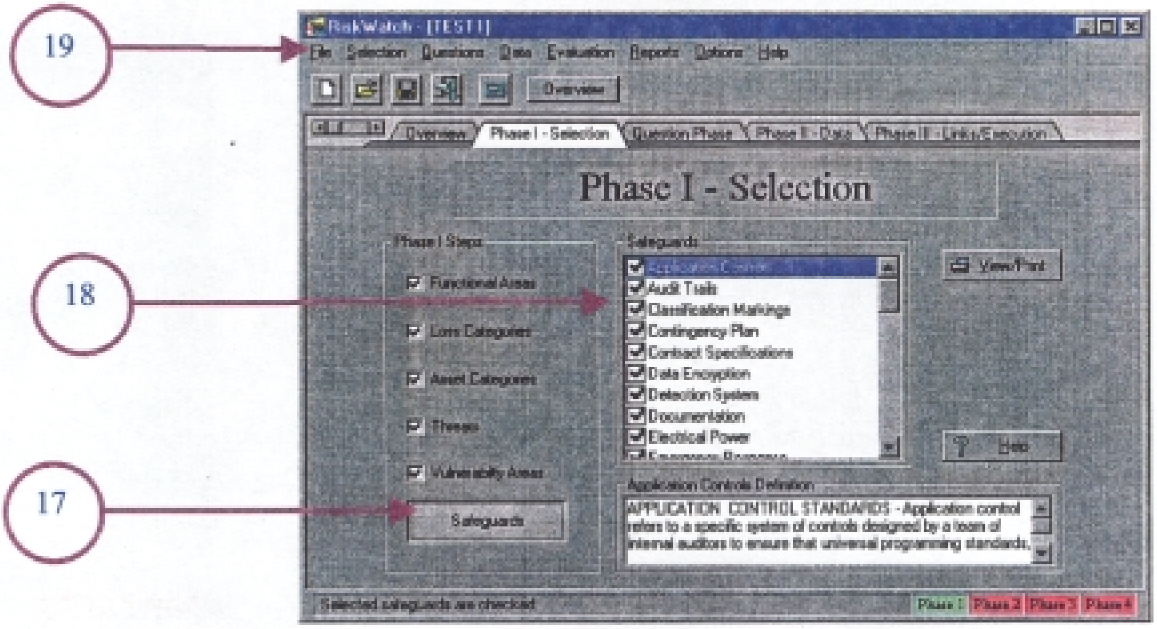
Selected vulnerability areas are checked.

Safeguards

17. **Click Safeguards** in the Phase I – Selection Tab.

18. **Click** on check mark in box to deselect a given Safeguard.

TIP
Later in the analysis, the analyst may decide to come back to this section and reselect or deselect more categories. It will not affect other data already entered.



Phase I Steps
☑ Functional Areas
☑ Loss Categories
☑ Asset Categories
☑ Threats
☑ Vulnerability Areas

Safeguards
☑ Application Controls
☑ Audit Trails
☑ Classification Markings
☑ Contingency Plan
☑ Contract Specifications
☑ Data Encryption
☑ Detection System
☑ Documentation
☑ Electrical Power

Application Controls Definition
APPLICATION CONTROL STANDARDS - Application control refers to a specific system of controls designed by a team of internal auditors to ensure that universal programming standards,

Selected safeguards are checked

19. Save case now by clicking on **File, Save.**

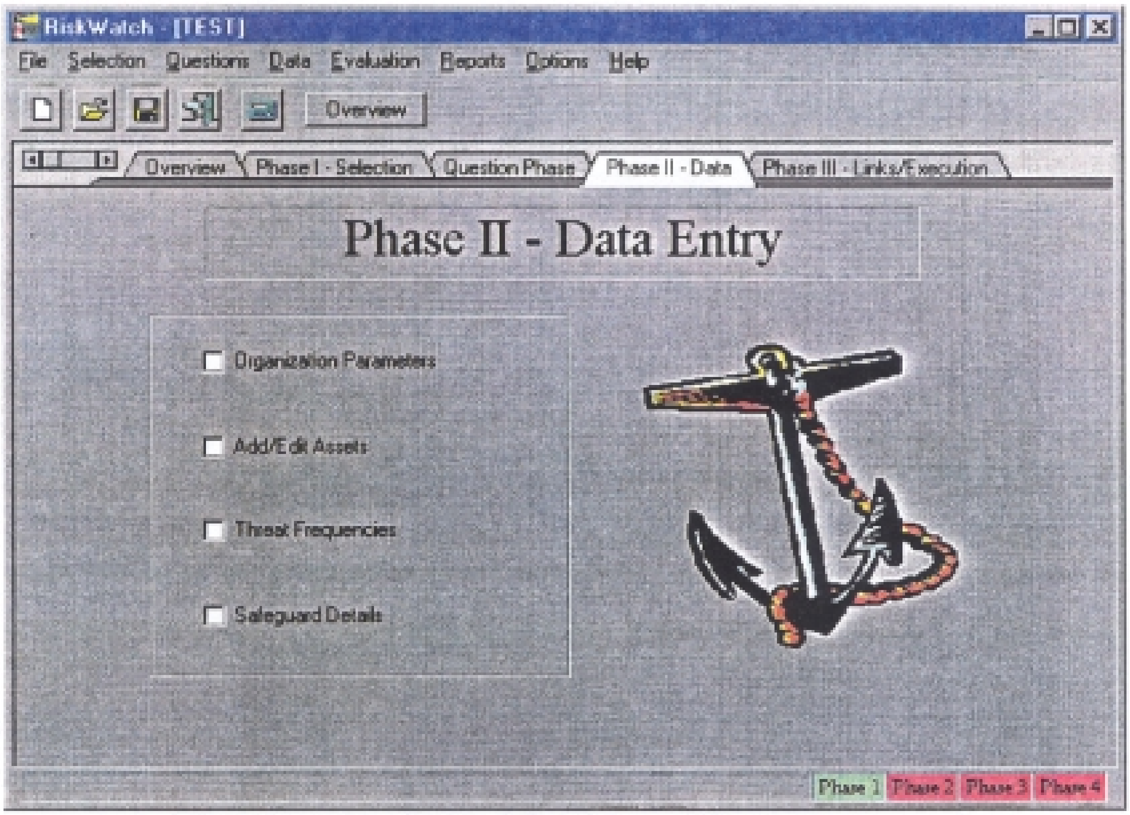
This concludes the tasks for Phase I, Selection.

Question Phase and Phase II

The Question Phase and Phase II can be performed simultaneously. For complete details on the Question Phase see Section 6 and Phase II - Data continues on next page.

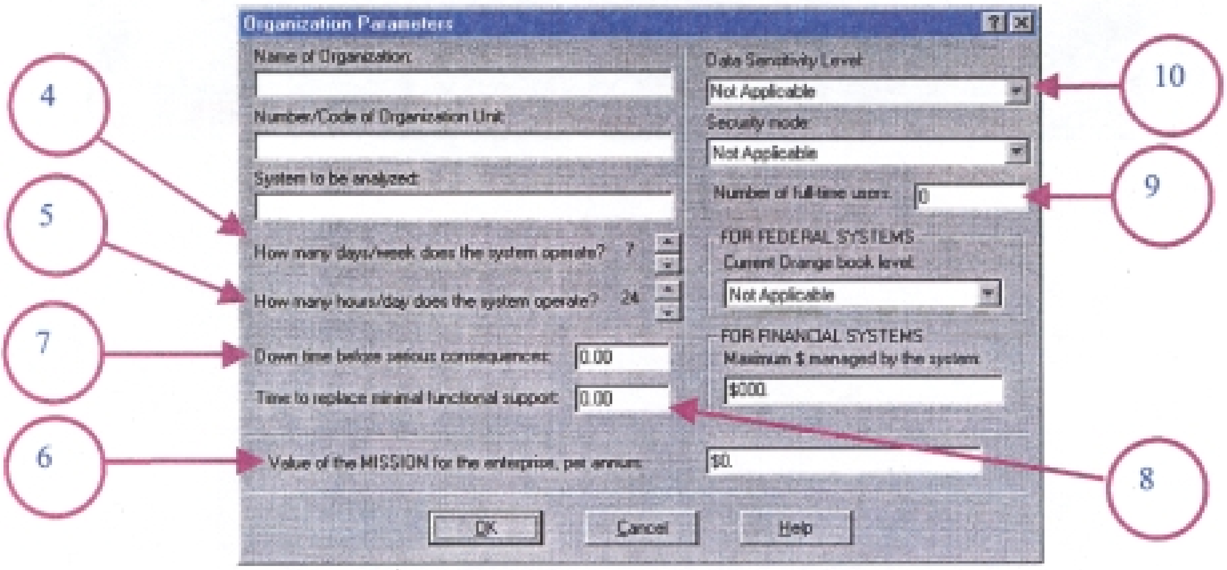
Phase II - Data

Phase II has four areas for data entry: Organization Parameters, Add/Edit Assets, Threat Frequencies, and Safeguard Details. Before entering the pertinent data, the analyst needs to review the data requirements for these areas from Section 4 and prepare the data for input into from RiskWatch. We recommended using screen prints as tools to assist in data collection. (Refer to Appendix A, How to Create Screen Prints on page 155 for how to make screen prints.)



Organization Parameters

1. If the case is closed, **Open** the review case following the steps in Opening An Existing Case on page 40. The Overview tab appears.
2. Select the Phase II – Data tab.
3. Select **Organization Parameters.** Input all data for the organization by tabbing from field to field. Refer to Section 4, Ideas For Collecting and Organizing Data, Organization Parameters on where/how to find or calculate this data.
4. How many days per week does the system operate? - **Enter** the **number of day** the business function operates.
5. How many hours per day does the system operate? - **Enter** the **number of hours** for business function.
6. All the remaining fields are used as background information only. Things to consider when inputting information for the following fields include:
7. Downtime before serious consequences. **Enter** the number of hours for business function.
8. Time to replace minimal functional support. - **Enter** the number of hours for business function.
9. Number of full-time equivalent (FTE) users. - **Enter** the number of employees for business function.
10. Data sensitivity level. - **Select** the appropriate level for business function.



Organization Parameters

Name of Organization:

Number/Code of Organization Unit:

System to be analyzed:

How many days/week does the system operate? 7

How many hours/day does the system operate? 24

Down time before serious consequences: 0.00

Time to replace minimal functional support: 0.00

Value of the MISSION for the enterprise, per annum: $0.

Data Sensitivity Level: Not Applicable

Security mode: Not Applicable

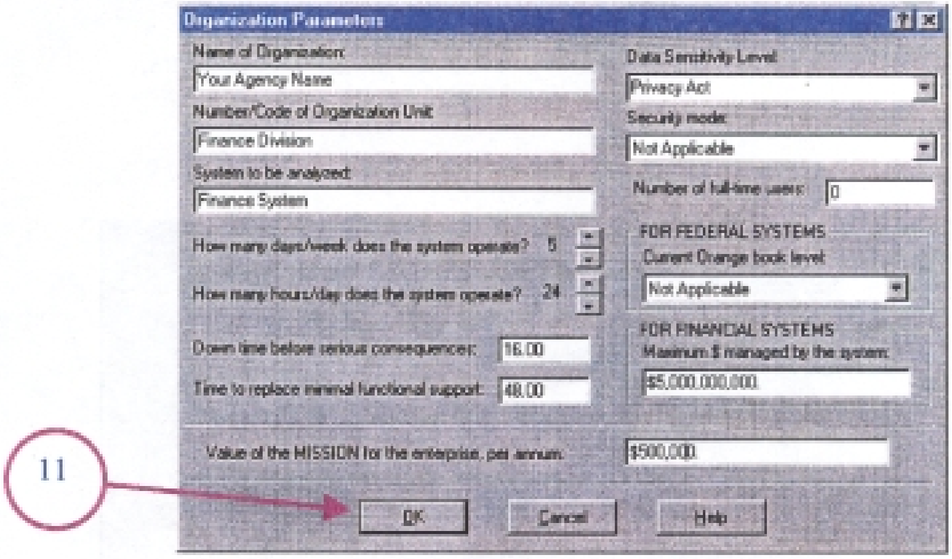
Number of full-time users: 0

FOR FEDERAL SYSTEMS
Current Orange book level: Not Applicable

FOR FINANCIAL SYSTEMS
Maximum $ managed by the system: $000.

11. Select **O.K.** This will returns to Phase II – Data Entry Tab.

12. **File, Save** to save the case.



Name of Organization: Your Agency Name

Number/Code of Organization Unit: Finance Division

System to be analyzed: Finance System

How many days/week does the system operate? 5

How many hours/day does the system operate? 24

Down time before serious consequences: 16.00

Time to replace minimal functional support: 48.00

Data Sensitivity Level: Privacy Act

Security mode: Not Applicable

Number of full-time users: 0

FOR FEDERAL SYSTEMS

Current Orange book level: Not Applicable

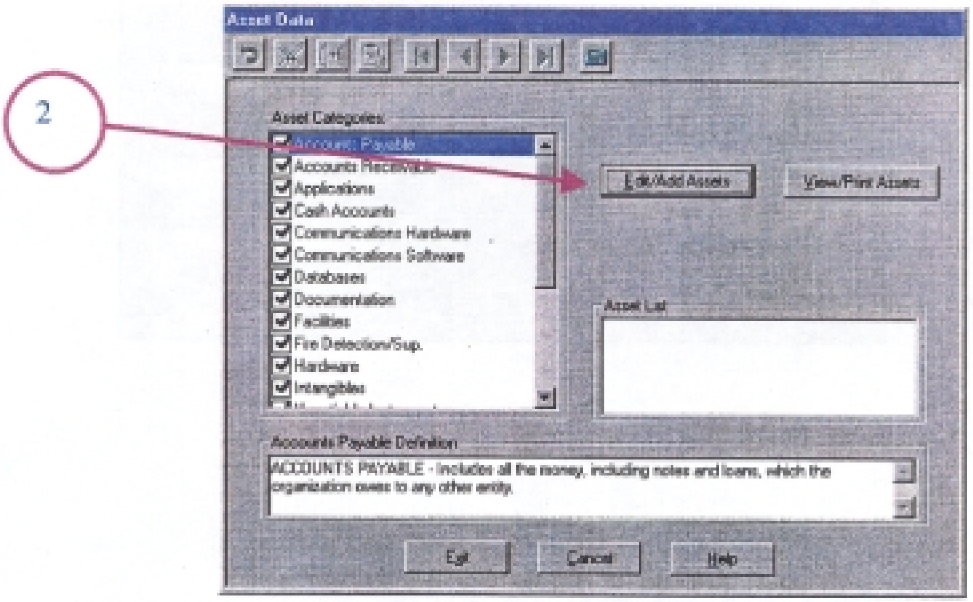
FOR FINANCIAL SYSTEMS

Maximum $ managed by the system: $5,000,000,000

Value of the MISSION for the enterpise, per annum: $500,000

Entering Assets And Their Values

1. Select **Add/Edit Assets** from the Phase II – Data tab. The Assets Data dialog box appears.
2. Select **Edit/Add Assets**. A different Assets Data dialog box appears.

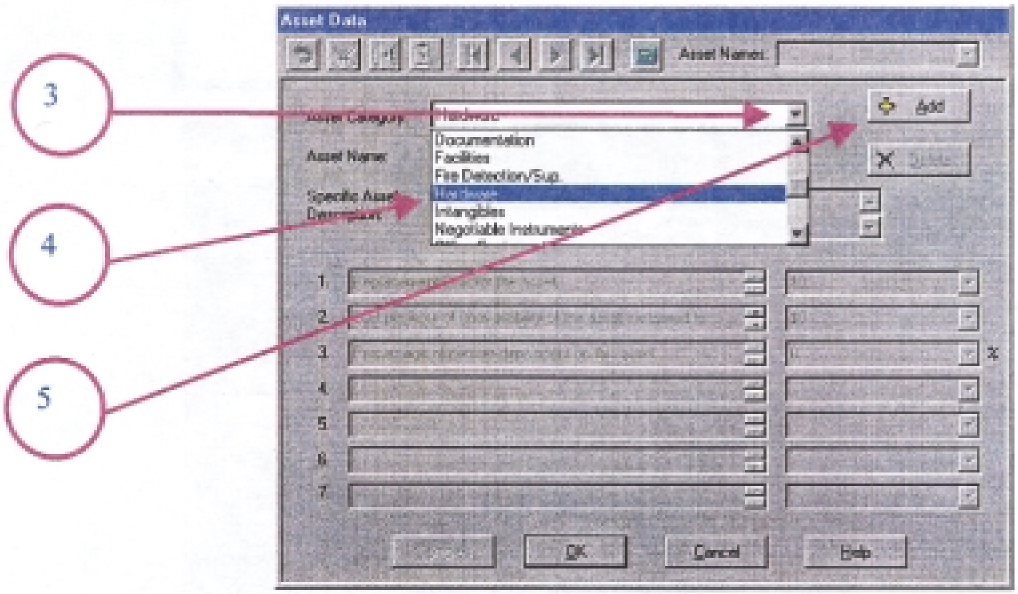


☑ Accounts Payable
☑ Accounts Receivable
☑ Applications
☑ Cash Accounts
☑ Communications Hardware
☑ Communications Software
☑ Databases
☑ Documentation
☑ Facilities
☑ Fire Detection/Sup.
☑ Hardware
☑ Intangibles

Accounts Payable Definition

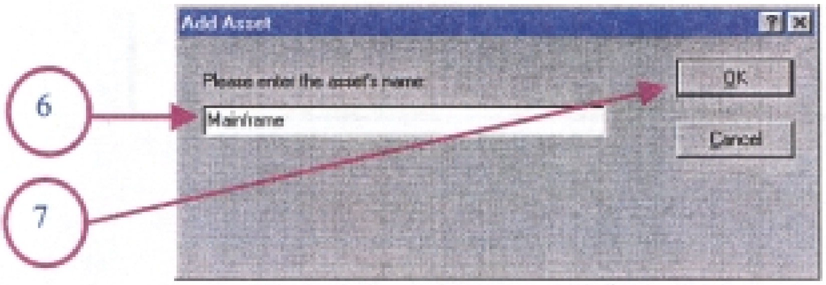
ACCOUNTS PAYABLE - Includes all the money, including notes and loans, which the organization owes to any other entity.

3. Select the **Assets Category** where data is to be entered by clicking once on the pull-down menu on the Asset Category box.
4. **Highlight** the Asset Category that needs to be add/edit.
5. Select +**Add** button. The Add Asset dialog box appear.



Asset Category: Hardware

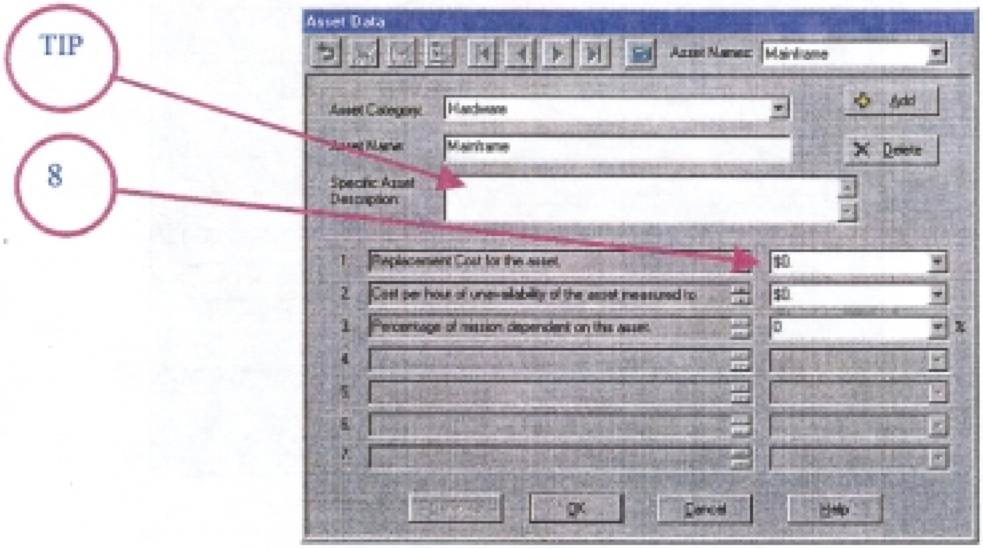
6. **Enter** the asset's name.
7. Select **O.K.** This will returns to the Asset Data dialog box.



Please enter the asset's name: Mainframe

8. **Enter** the appropriate asset values in the boxes as requested by RiskWatch. Refer to Section 4, Ideas For Collecting and Organizing Data, Add/Edit Assets on how/where to determine these values.

TIP
Entering the asset description or detailed asset information into in the 'Specific Asset Description' box is optional.



Asset Name: Mainframe

Asset Category: Hardware

Asset Name: Mainframe

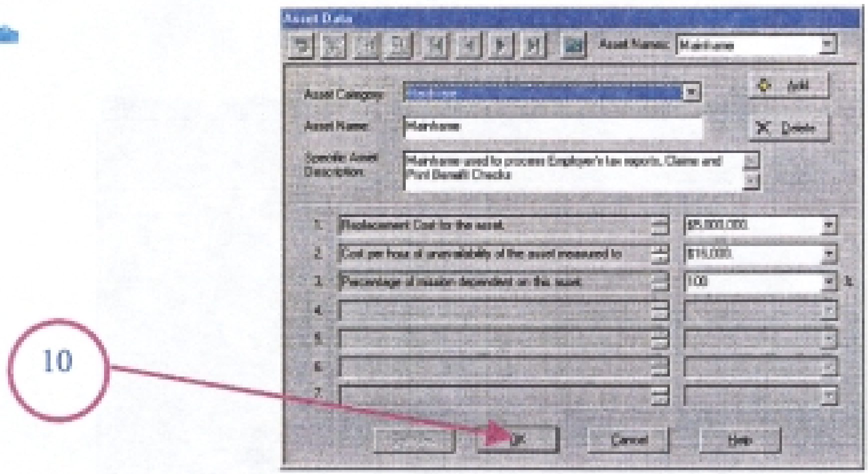
Specific Asset Description:

1. Replacement Cost for the asset. $0.
2. Cost per hour of unavailability of the asset measured to $0.
3. Percentage of mission dependent on the asset. 0 %
4.
5.
6.
7.

9. Continue adding assets using step 3 to 8 until all assets have been entered. If finished entering all assets or returning to save, proceed to step 10.

WARNING
SAVE OFTEN TO AVOID LOSS OF COMPLETED WORK.

10. Select **O.K.**



Asset Name: Mainframe

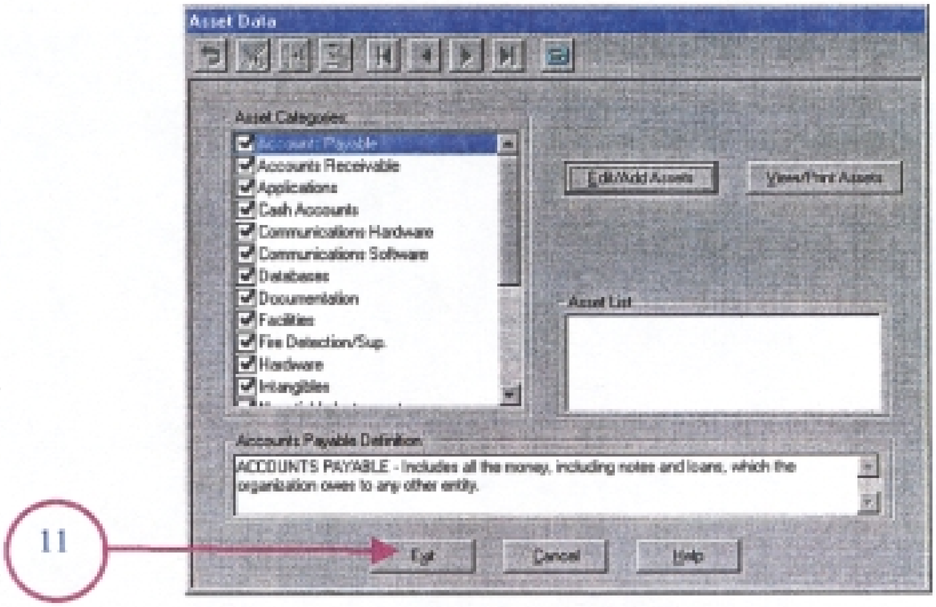
Asset Category: Hardware

Asset Name: Mainframe

Specific Asset Description: Mainframe used to process Employer's tax reports, Claims and Print Benefit Checks

1.	Replacement Cost for the asset.	$5,000,000
2.	Cost per hour of unavailability of the asset measured to	$15,000
3.	Percentage of mission dependent on the asset.	100 %
4.		
5.		
6.		
7.		

11. Select **Exit** to return to Phase II – Data Tab.



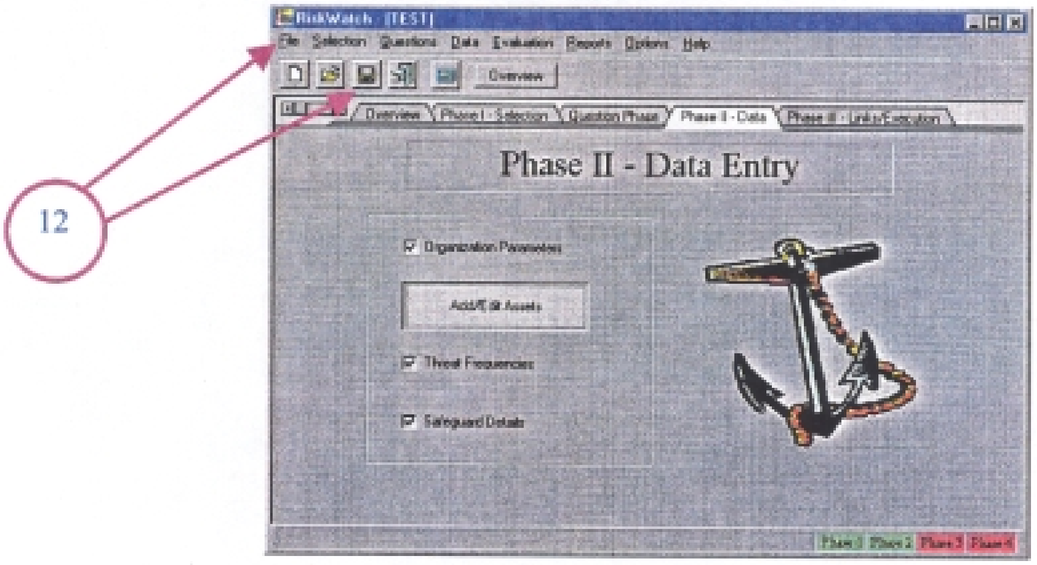
Asset Categories:

☑ Accounts Payable
☑ Accounts Receivable
☑ Applications
☑ Cash Accounts
☑ Communications Hardware
☑ Communications Software
☑ Databases
☑ Documentation
☑ Facilities
☑ Fire Detection/Sup.
☑ Hardware
☑ Intangibles

Accounts Payable Definition:

ACCOUNTS PAYABLE - Includes all the money, including notes and loans, which the organization owes to any other entity.

12. Then **File, Save**, or click on save icon. To complete the entering of assets, return to step 1. If all assets are entered, continue to Changing Threat Frequencies on the next page.



Phase II - Data Entry

☑ Organization Parameters

☑ Threat Frequencies

☑ Safeguard Details

Changing Threat Frequencies

WARNING
If a Threat is deselected in Phase I, this Threat will not be listed under Selected Threat. See discussion in Ideas For Collecting and Organizing Data on Threat Frequency on page 25.

1 If the case is closed, **Open** the review case following the steps in Opening An Existing Case on page 40. The Overview tab appears.

2 If in either the Overview or the Phase II – Data tab, click **Threat Frequencies**. The Phase II – Threat Frequencies dialog box appears.

Using the information gathered in Section 4, change the LAFE to reflect the conditions of the business function.

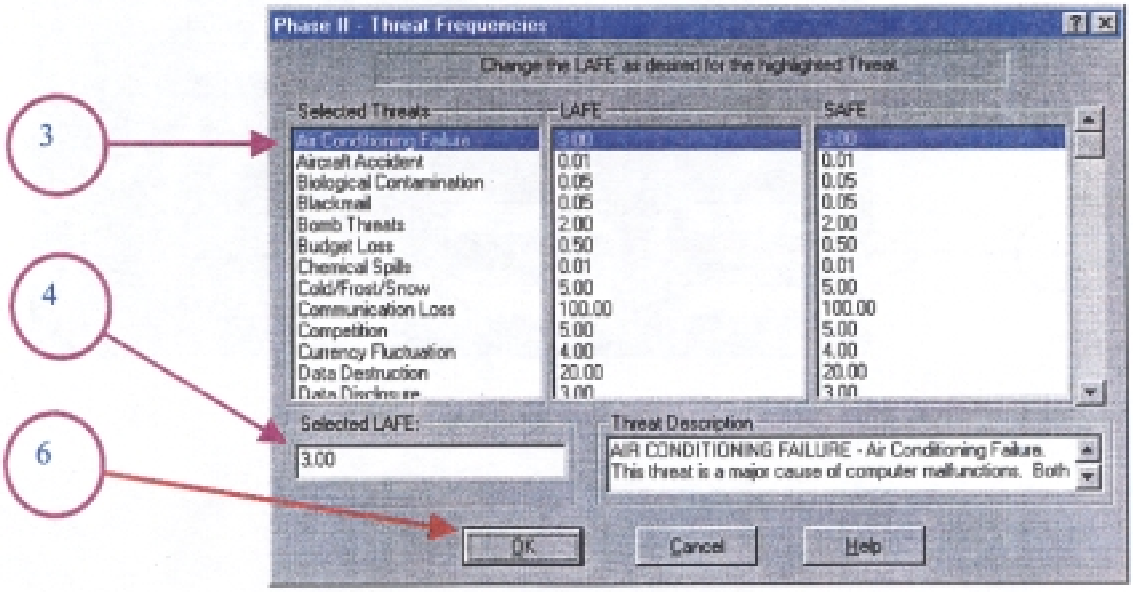
TIP:
The analyst may only adjust the LAFE column. If unsure, use the SAFE provided in RiskWatch.

3 **Highlight** the threat in Selected Threats column that needs changing.

4 RiskWatch will place the cursor in the Selected LAFE box. Enter the new LAFE.

5 Repeat step 3 and 4 until all LAFEs are changed, then continue to step 6.

6 Click **O.K.** This will return to the Phase II - Data tab. **Save** the case.



Phase II - Threat Frequencies

Change the LAFE as desired for the highlighted Threat.

Selected Threats	LAFE	SAFE
Air Conditioning Failure	3.00	3.00
Aircraft Accident	0.01	0.01
Biological Contamination	0.05	0.05
Blackmail	0.05	0.05
Bomb Threats	2.00	2.00
Budget Loss	0.50	0.50
Chemical Spills	0.01	0.01
Cold/Frost/Snow	5.00	5.00
Communication Loss	100.00	100.00
Competition	5.00	5.00
Currency Fluctuation	4.00	4.00
Data Destruction	20.00	20.00
Data Disclosure	3.00	3.00

Selected LAFE: 3.00

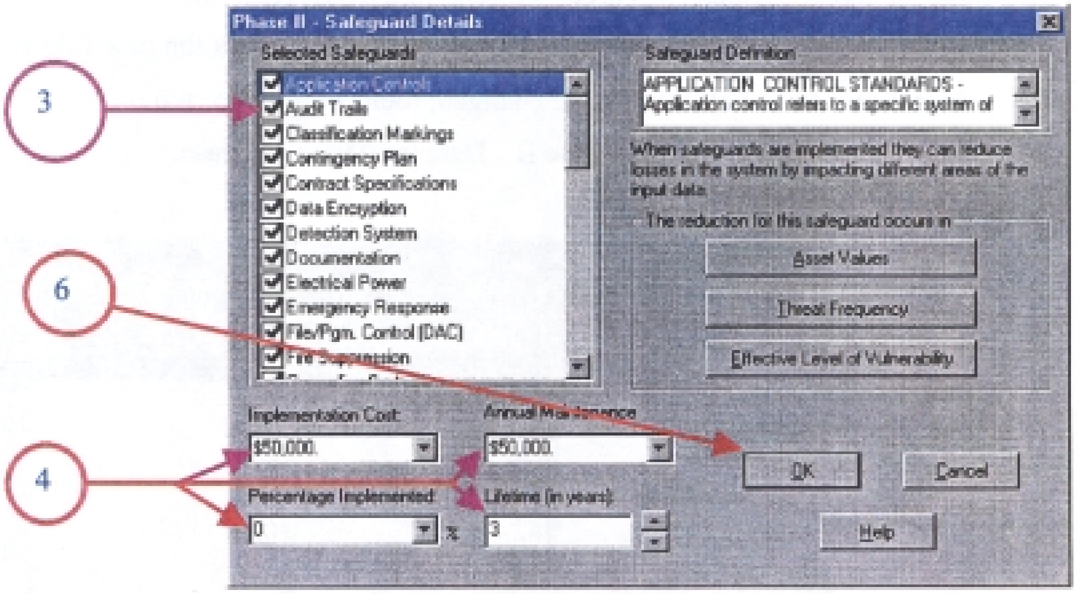
Threat Description
AIR CONDITIONING FAILURE - Air Conditioning Failure. This threat is a major cause of computer malfunctions. Both

Safeguard Details

In Safeguard Details, enter the information on the safeguards identified in Section 4 that your agency has either partially or completely implemented.

> WARNING
> If a Safeguard was deselected in Phase I, this safeguard will not be listed under Selected Safeguards. See discussion on Safeguard Details on page 26.

1. If the case is closed, **Open** the review case following the steps in Opening An Existing Case on page 40. The Overview tab appears.
2. If in either the Overview or the Phase II – Data tab, **Click Safeguard Details**. The Phase II - Safeguard Details dialog box appears.
3. Highlight a safeguard from **Selected Safeguards** box.
4. Enter the Implementation Cost, Annual Maintenance Cost, Lifetime, and the Percentage Implemented tabbing from field to field.
5. Repeat step 3 and 4 until all applicable safeguards are entered, then continue to step 6.
6. Select **O.K. Save** the case now.


Phase II - Safeguard Details
3
6
4
Asset Values
Threat Frequency
Effective Level of Vulnerability
OK
Cancel
Help

Selected Safeguards

- ☑ Application Controls
- ☑ Audit Trails
- ☑ Classification Markings
- ☑ Contingency Plan
- ☑ Contract Specifications
- ☑ Data Encryption
- ☑ Detection System
- ☑ Documentation
- ☑ Electrical Power
- ☑ Emergency Response
- ☑ File/Pgm. Control (DAC)
- ☑ Fire Suppression

Safeguard Definition

APPLICATION CONTROL STANDARDS - Application control refers to a specific system of

When safeguards are implemented they can reduce losses in the system by impacting different areas of the input data.

The reduction for this safeguard occurs in

Implementation Cost: $50,000.

Annual Maintenance: $50,000.

Percentage Implemented: 0 %

Lifetime (in years): 3

Reduction for This Safeguard Occurs In

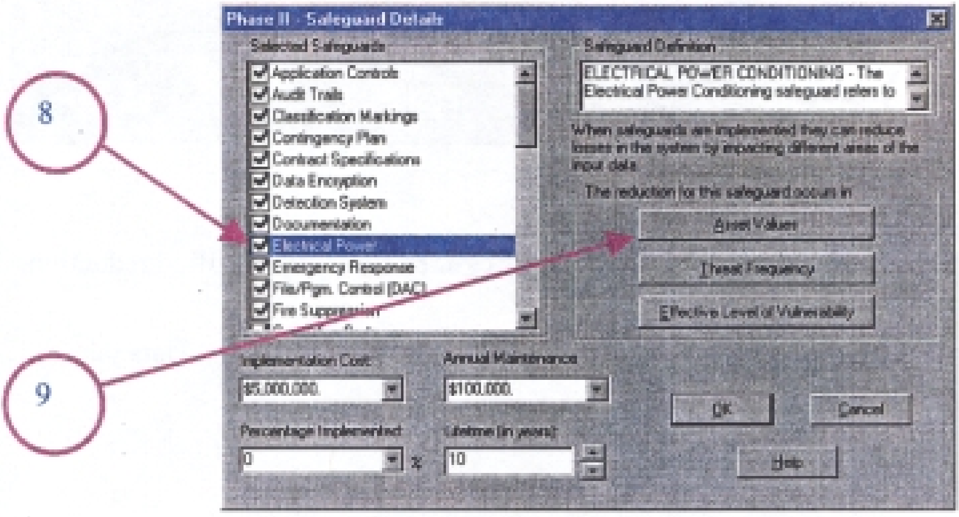
Using the Reduction for this Safeguard Occurs In fields is optional. Only the experienced RiskWatch user should change the RiskWatch defaults.

> WARNING
> Due to the complexity and level of effort required to change these percentages, it is ***strongly*** recommend that RiskWatch default values be used.

7. If in either the Overview or the Phase II – Data tab, Click **Safeguard Details**. The Phase II - Safeguard Details dialog box appears.
8. Highlight the safeguard in the **Selected Safeguards** column.

Asset Values

9. Select **Asset Values** button.



ELECTRICAL POWER CONDITIONING - The Electrical Power Conditioning safeguard refers to

When safeguards are implemented they can reduce losses in the system by impacting different areas of the input data

The reduction for this safeguard occurs in

Implementation Cost: $5,000,000.

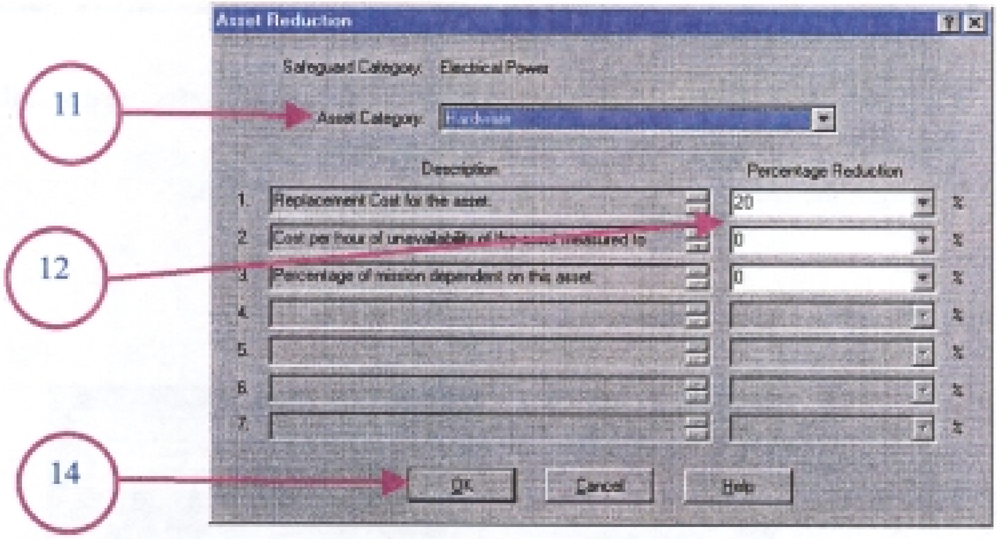
Annual Maintenance: $100,000.

Percentage Implemented: 0 %

Lifetime (in years): 10

10. The **Asset Reduction** dialog box appears.

11. Select the **Asset Category** that needs to be reduced by clicking on the pull-down menu to the right of **Asset Category**.
12. Enter the **Percentage of Reduction** for each applicable **Description**.
13. Continue selecting the **Asset Category** for reduction until all identified reductions are completed for the selected **Safeguard Category**.
14. Select **O.K.**



Safeguard Category: Electrical Power

Asset Category: Hardware

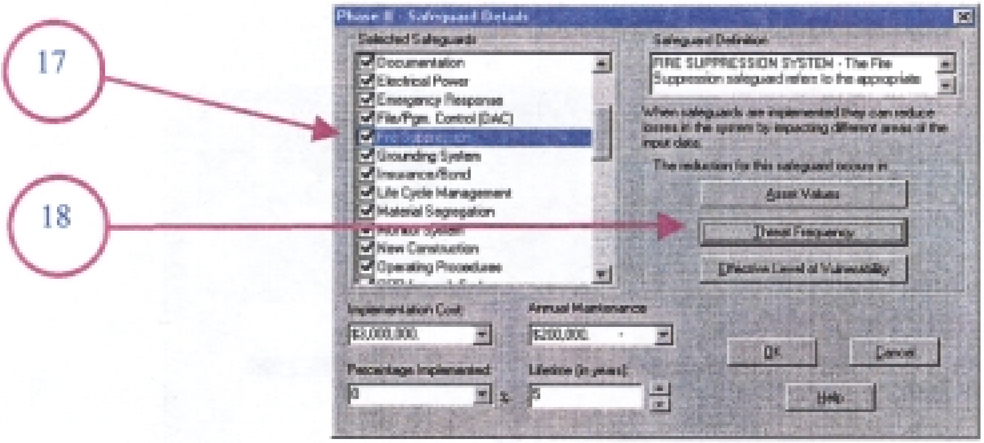
	Description	Percentage Reduction	
1.	Replacement Cost for the asset.	20	%
2.	Cost per hour of unavailability of the asset measured to	0	%
3.	Percentage of mission dependent on this asset.	0	%
4.			%
5.			%
6.			%
7.			%

15. Repeat Steps 11 to 14 for each **Selected Safeguard** until all identified reductions are entered for under **Asset Values**.
16. **Save** by clicking **O.K.**, then **O.K.** again. This returns to Phase II – Data tab.

Threat Frequency

17. Highlight the safeguard in the **Selected Safeguards** column.

18. Select **Threat Frequency button**. The **Safeguard Reduction** dialog box appears.



Phase II - Safeguard Details

Selected Safeguards

- ☑ Documentation
- ☑ Electrical Power
- ☑ Emergency Response
- ☑ File/Pgm. Control (DAC)
- ☑ Fire Suppression
- ☑ Grounding System
- ☑ Insurance/Bond
- ☑ Life Cycle Management
- ☑ Material Segregation
- ☑ Monitor System
- ☑ New Construction
- ☑ Operating Procedures

Safeguard Definition

FIRE SUPPRESSION SYSTEM - The Fire Suppression safeguard refers to the appropriate

When safeguards are implemented they can reduce losses in the system by impacting different areas of the input data.

The reduction for this safeguard occurs in:

Implementation Cost: $3,000,000.

Annual Maintenance: $200,000.

Percentage Implemented: 0 %

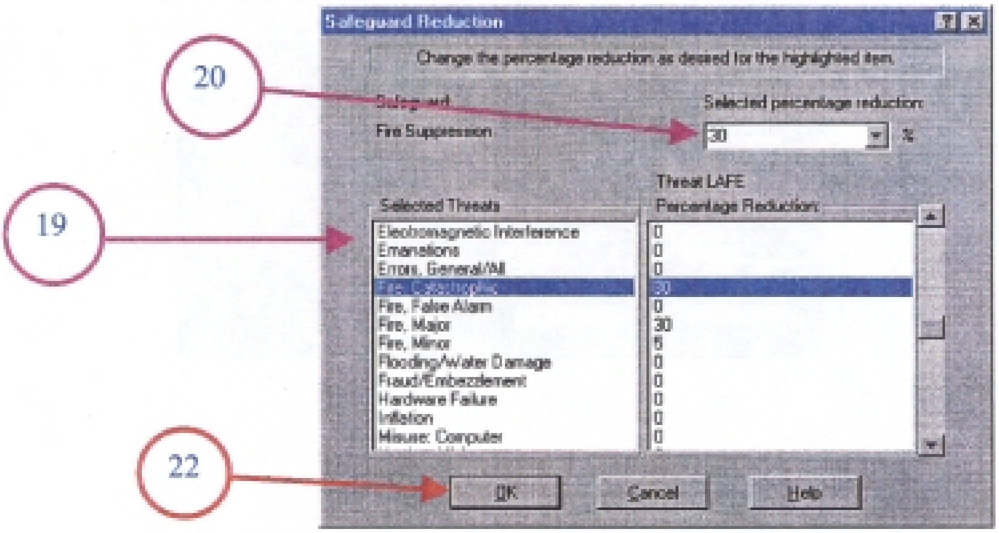
Lifetime (in years): 5

19. Highlight the threat to be reduced in the **Selected Threats** column

20. Select the percentage of reduction from the **Selected percentage reduction** pull-down menu.

21. Continue selecting the **Threat** for reduction until all changes are completed for this selected **Safeguard Category**.

22. Select **O.K.**



Change the percentage reduction as desired for the highlighted item.

Safeguard
Fire Suppression

Selected percentage reduction: 30 %

Selected Threats	Threat LAFE Percentage Reduction:
Electromagnetic Interference	0
Emanations	0
Errors, General/All	0
Fire, Catastrophic	30
Fire, False Alarm	0
Fire, Major	30
Fire, Minor	5
Flooding/Water Damage	0
Fraud/Embezzlement	0
Hardware Failure	0
Inflation	0
Misuse: Computer	0

23. Repeat Steps 19 to 22 for each **Selected Safeguard** until all identified reductions are completed under **Threat Frequencies**.

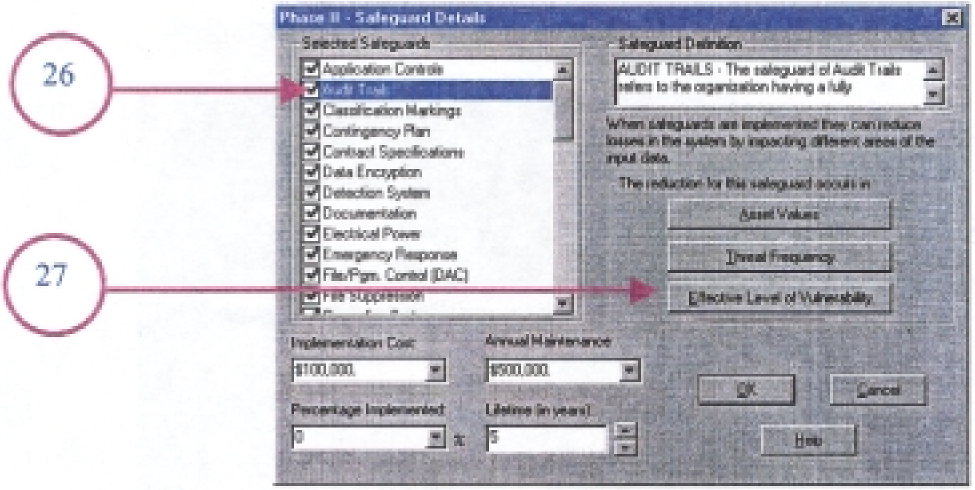
24. To **Save** click **O.K.**, then **O.K.** again. This returns to Phase II – Data tab.

25. **File, Save**.

Effective Level of Vulnerability

26. Highlight the safeguard in the **Selected Safeguards** column.

27. Select the **Effective Level of Vulnerability** button. The **Safeguard Reduction** dialog box appears.



AUDIT TRAILS - The safeguard of Audit Trails refers to the organization having a fully

When safeguards are implemented they can reduce losses in the system by impacting different areas of the input data.

The reduction for this safeguard occurs in

Implementation Cost: $100,000.

Annual Maintenance: $500,000.

Percentage Implemented: 0 %

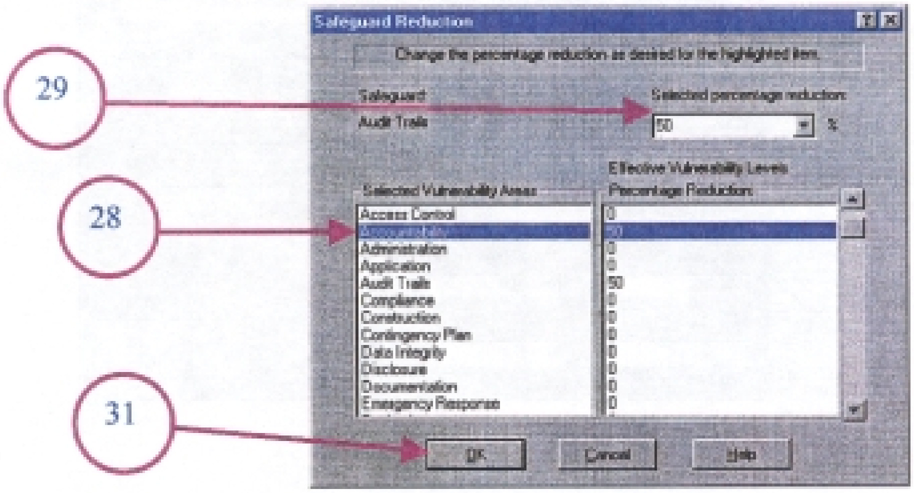
Lifetime (in years): 5

28. Highlight the vulnerability to be reduced in the **Selected Vulnerability Areas** column.

29. Select the percentage reduction from the **Selected percentage reductions** pull-down menu.

30. Continue selecting the vulnerability for each reduction until all identified reductions have been entered for the **Selected Safeguard**.

31. Select **OK.**



Change the percentage reduction as desired for the highlighted item.

Safeguard: Audit Trails

Selected percentage reduction: 50 %

Selected Vulnerability Areas	Effective Vulnerability Levels Percentage Reduction
Access Control	0
Accountability	50
Administration	0
Application	0
Audit Trails	50
Compliance	0
Construction	0
Contingency Plan	0
Data Integrity	0
Disclosure	0
Documentation	0
Emergency Response	0

32. Repeat Steps 28 to 31 for each **Selected Safeguard** until all identified reductions are completed for the **Effective Level of Vulnerability**.

33. To Save, click **OK**, then **OK** again. This returns to Phase II – Data tab.

34. **File, Save**.

This concludes the tasks for Phase II, Data.

Phase III - Relationships and Program Execution

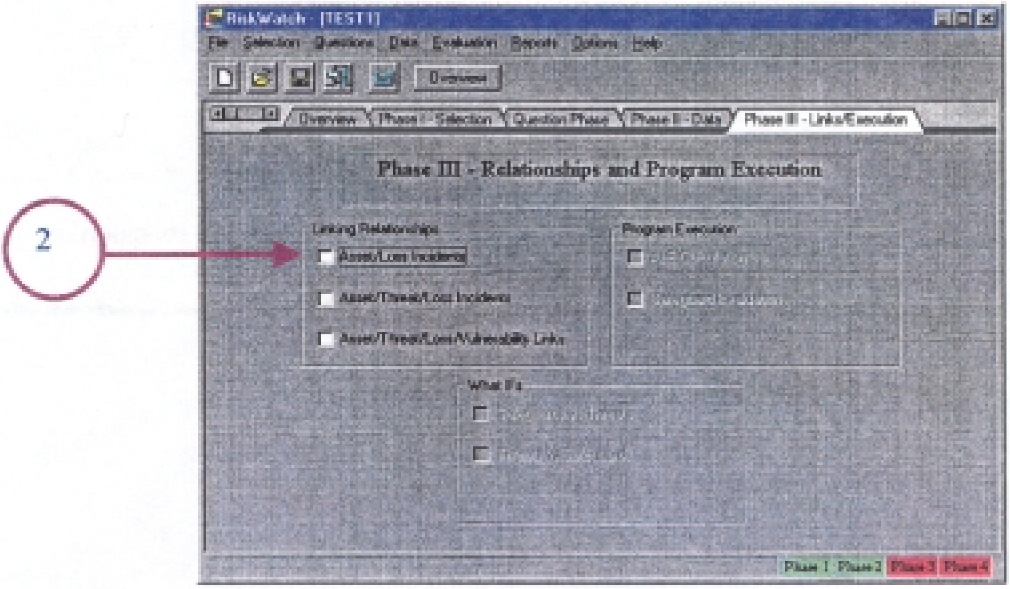
In Phase III, the analyst reviews the default relationships established by RiskWatch between assets, threats, losses, and vulnerabilities. Only advanced users should make changes. This phase has three activities: linking relationships, ALE calculation, and safeguard evaluation.

Linking Relationships

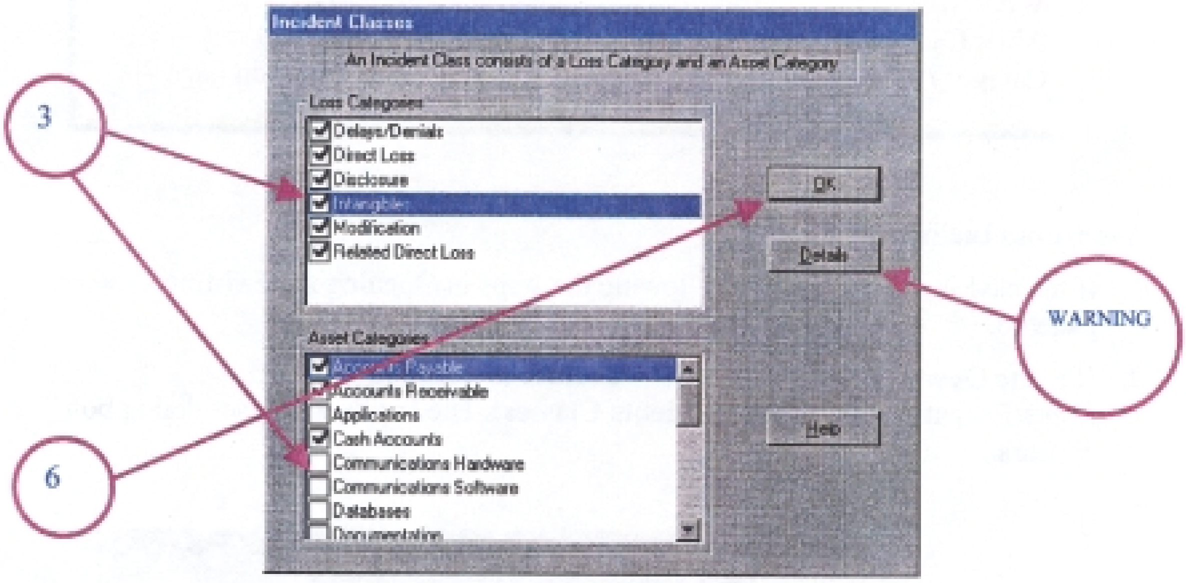
WARNING
Asset Categories are deselected in Phase I. If an additional Asset Category is needed, return to Phase I. See Asset Categories on page 46.

Asset/Loss Incidents

1. If the case is closed, Open it following the steps in Opening An Existing Case on page 40.
2. If at the Overview tab or **Asset/Loss Incidents** from the Phase III – Links/Execution tab, select **Incidents Classes**. The Incident Classes dialog box appears.


2
RiskWatch - [TEST1]
File Selection Questions Data Evaluation Reports Options Help
Overview
Overview
Phase I - Selection
Question Phase
Phase II - Data
Phase III - Links/Execution
Phase III - Relationships and Program Execution
Linking Relationships
□ Asset/Loss Incidents
□ Asset/Threat/Loss Incidents
□ Asset/Threat/Loss/Vulnerability Links
Program Execution
What If's
Phase 1
Phase 2
Phase 3
Phase 4

3. Review the links between the **Loss Categories** and the **Asset Categories**. To select an additional asset, highlight the **Loss Category** to which the asset will be added.
4. Click the box to left of **Asset Category** for selection. Repeat until all appropriate assets are linked to the selected **Loss Category**.
5. Select the next **Loss Category** and repeat Steps 3 to 4 until the analyst establish all the new links between asset and loss categories.
6. Click **OK** to return to the Phase III tab.



Incident Classes

An Incident Class consists of a Loss Category and an Asset Category

Loss Categories

☑ Delays/Denials
☑ Direct Loss
☑ Disclosure
☑ Intangibles
☑ Modification
☑ Related Direct Loss

Asset Categories

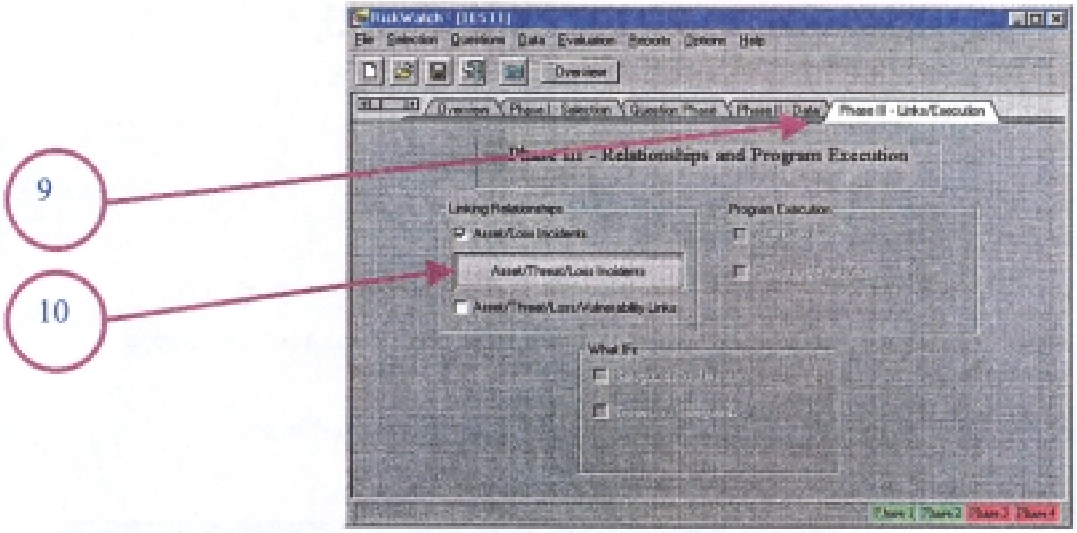
☑ Accounts Payable
☑ Accounts Receivable
☐ Applications
☑ Cash Accounts
☐ Communications Hardware
☐ Communications Software
☐ Databases
☐ Documentation

WARNING
The **Detail** button reveals the formulas that RiskWatch uses in its calculations.
NEVER ALTER THESE FORMULAS.

7. **File, Save**

Asset/Threat/Loss Incidents

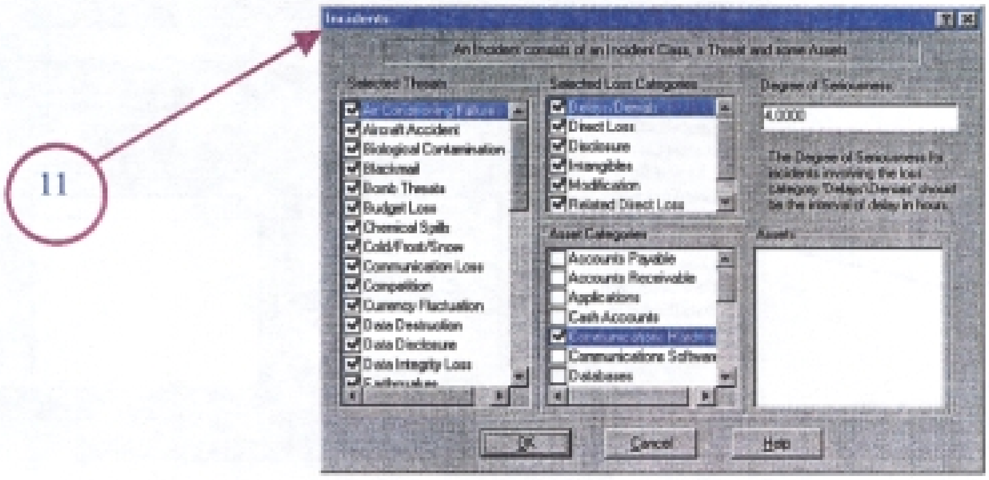
8. If the case is closed, Open it following the steps in Opening An Existing Case on page 40.
9. Click **Phase III – Links and Execution** tab.
10. Select **Asset/Threats/Loss Incidents.**


9
10
RiskWatch - [TEST]
File Selection Questions Data Evaluation Reports Options Help
Overview
Overview
Phase I - Selection
Question Phase
Phase II - Data
Phase III - Links/Execution
Phase III - Relationships and Program Execution
Linking Relationships
Asset/Threat/Loss Incidents
Program Execution
What If
Phase 1
Phase 2
Phase 3
Phase 4

☑ Asset/Loss Incidents

□ Asset/Threat/Loss/Vulnerability Links

11. The Incidents dialog box appears.



An Incident consists of an Incident Class, a Threat and some Assets

Selected Threats

☑ Air Conditioning Failure
☑ Aircraft Accident
☑ Biological Contamination
☑ Blackmail
☑ Bomb Threats
☑ Budget Loss
☑ Chemical Spills
☑ Cold/Frost/Snow
☑ Communication Loss
☑ Competition
☑ Currency Fluctuation
☑ Data Destruction
☑ Data Disclosure
☑ Data Integrity Loss
☑ Earthquakes

Selected Loss Categories

☑ Delays/Denials
☑ Direct Loss
☑ Disclosure
☑ Intangibles
☑ Modification
☑ Related Direct Loss

Degree of Seriousness: 4.0000

The Degree of Seriousness for incidents involving the loss category 'Delays/Denials' should be the interval of delay in hours.

Asset Categories

□ Accounts Payable
□ Accounts Receivable
□ Applications
□ Cash Accounts
☑ Communications Hardware
□ Communications Software
□ Databases

Assets

WARNING:
If changes are determined necessary in the Threats or Loss Categories columns, return to Phases I and II. A complete Asset Category may be deselected; however, this is not recommended. Deselect only single assets **from** the **Assets** box. If, later, a single asset reselected, ALL links must be manually reestablished. If the analyst chooses to experiment, he/she should save to another case and experiment there.

To Change Degree of Seriousness

Optional

> WARNING
> Return to discussion on Phase III before applying changes.
> Also refer to Appendix A, Incident Degree of Seriousness
> for a listing of default SEs for each incident.

12. Highlight a threat from the **Selected Threats** box.

13. Highlight a loss from the **Selected Loss Categories** box.

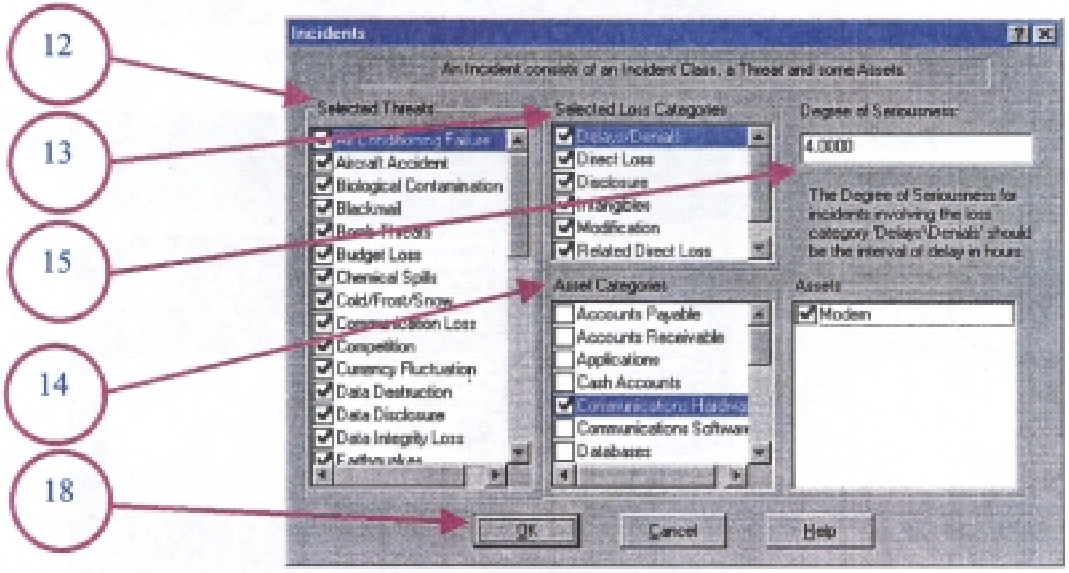
14. Highlight an asset from the **Asset Categories** box.

15. Place cursor in **Degree of Seriousness** box.

16. Delete the default number and enter the new **Degree of Seriousness**.

17. Repeated step 12 to 16 for each additional **Degree of Seriousness** that needs changing.

18. **Click O.K.**, when all Degree of Seriousness changes has been made.



An Incident consists of an Incident Class, a Threat and some Assets.

Degree of Seriousness: 4.0000

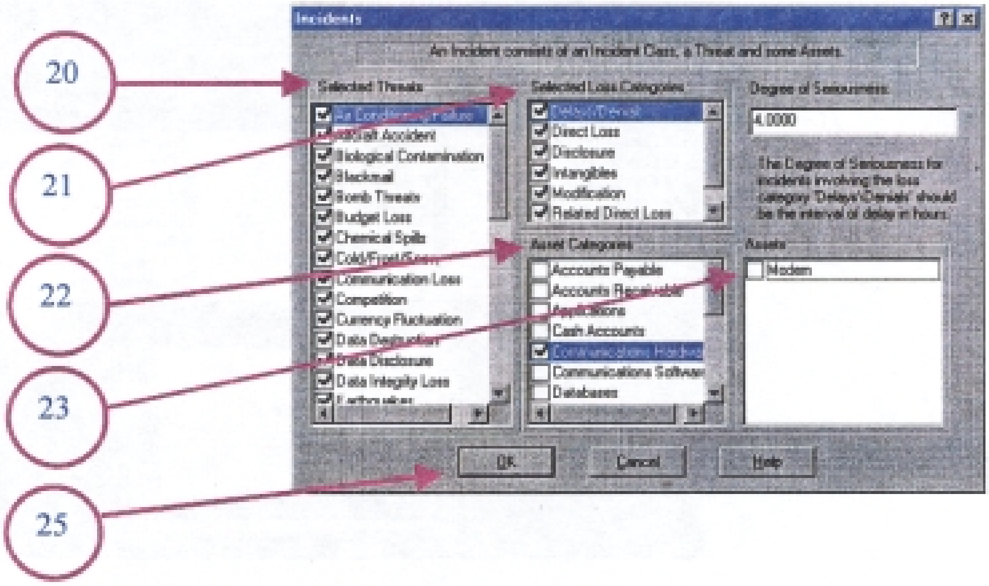
The Degree of Seriousness for incidents involving the loss category 'Delays\Denials' should be the interval of delay in hours.

19. **Save the case.**

To Deselect an Asset

(Optional)

20. Highlight a threat from the **Selected Threats** box.
21. Highlight a loss from the **Selected Loss Categories** box.
22. Highlight an asset from the **Asset Categories** box.
23. Click box next to the desired asset in the **Assets** column that needs to be deselected. Click **once**. This should remove check mark.



An Incident consists of an Incident Class, a Threat and some Assets.

Selected Threats
- ☑ Air Conditioning Failure
- ☑ Aircraft Accident
- ☑ Biological Contamination
- ☑ Blackmail
- ☑ Bomb Threats
- ☑ Budget Loss
- ☑ Chemical Spills
- ☑ Cold/Frost/Snow
- ☑ Communication Loss
- ☑ Competition
- ☑ Currency Fluctuation
- ☑ Data Destruction
- ☑ Data Disclosure
- ☑ Data Integrity Loss
- ☑ Earthquakes

Selected Loss Categories
- ☑ Delays/Denials
- ☑ Direct Loss
- ☑ Disclosure
- ☑ Intangibles
- ☑ Modification
- ☑ Related Direct Loss

Degree of Seriousness: 4.0000

The Degree of Seriousness for incidents involving the loss category 'Delays\Denials' should be the interval of delay in hours.

Asset Categories
- □ Accounts Payable
- □ Accounts Receivable
- □ Applications
- □ Cash Accounts
- ☑ Communications Hardware
- □ Communications Software
- □ Databases

Assets
- □ Modem

24. Repeated step 20 to 23 for each additional asset that need deselecting.
25. Click **OK** after completing all changes.
26. **Save** the case.

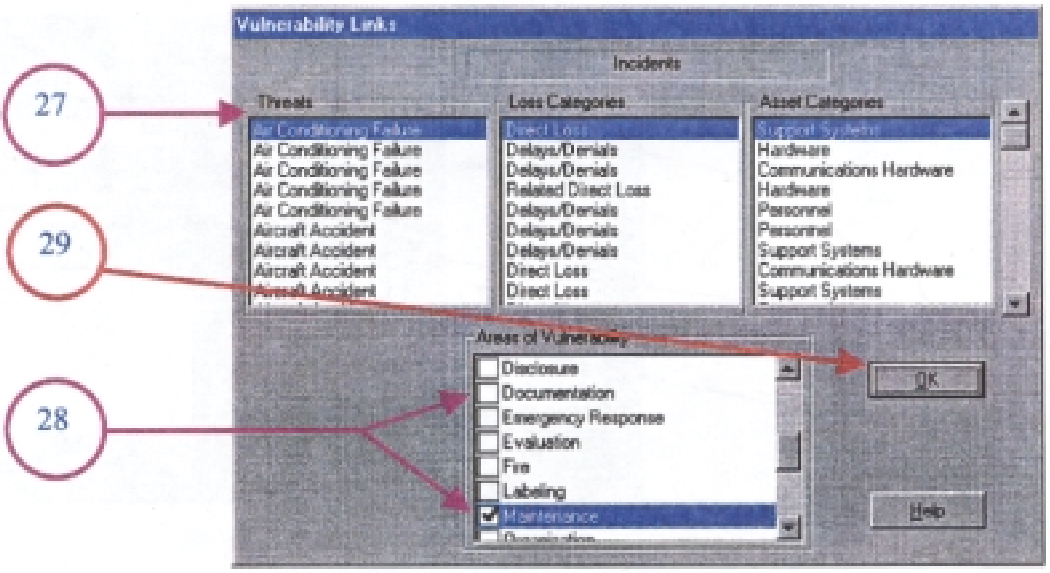
Asset/Threat/Loss/Vulnerability Links

(Optional)

27. Highlight an **Incident**.

28. To delete or create a link, click once on the box next to the vulnerability in the **Areas of Vulnerability** box.

29. Click **OK** after making all the changes.



Incidents

Threats	Loss Categories	Asset Categories
Air Conditioning Failure	Direct Loss	Support Systems
Air Conditioning Failure	Delays/Denials	Hardware
Air Conditioning Failure	Delays/Denials	Communications Hardware
Air Conditioning Failure	Related Direct Loss	Hardware
Air Conditioning Failure	Delays/Denials	Personnel
Aircraft Accident	Delays/Denials	Personnel
Aircraft Accident	Delays/Denials	Support Systems
Aircraft Accident	Direct Loss	Communications Hardware
Aircraft Accident	Direct Loss	Support Systems

Areas of Vulnerability

□ Disclosure
□ Documentation
□ Emergency Response
□ Evaluation
□ Fire
□ Labeling
☑ Maintenance

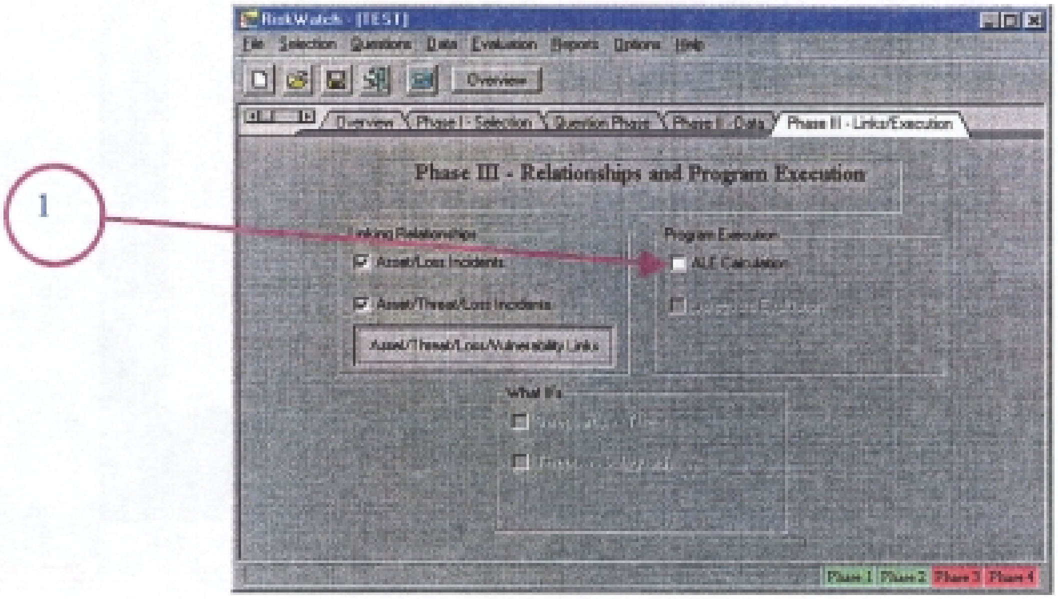
30. **Save** the case.

Program Execution

After completing Phases I and II and establishing Linking Relationships, RiskWatch allows the analyst to calculate the Annual Loss Expectancy (ALE) and Safeguard Evaluation.

Annual Loss Expectancy (ALE)

1. Click **ALE Calculation.**


1
RiskWatch - [TEST]
File Selection Questions Data Evaluation Reports Options Help
Overview
Overview
Phase I - Selection
Question Phase
Phase II - Data
Phase III - Links/Execution
Phase III - Relationships and Program Execution
Linking Relationships
Program Execution
Asset/Threat/Loss/Vulnerability Links
What If's
Phase 1
Phase 2
Phase 3
Phase 4

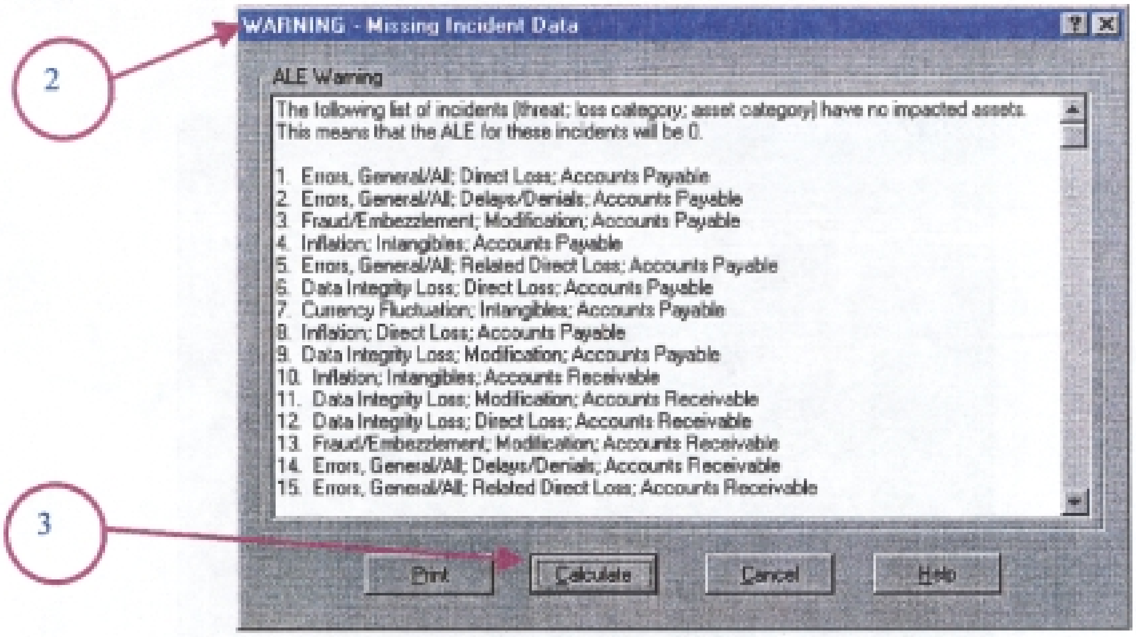
☑ Asset/Loss Incidents

☑ Asset/Threat/Loss Incidents

□ ALE Calculation

2. An **ALE Warning - Missing Incident Data** dialog box may appear after RiskWatch completes the calculation. Check each incident message and correct, if possible. These corrections will most likely occur in Phase III, under Asset/Threat/Loss Incidents. After making the corrections, repeat the steps for Asset/Threat/Loss/Vulnerability Links.

3. When comfortable that all error messages have been corrected, then click the **Calculate** button.



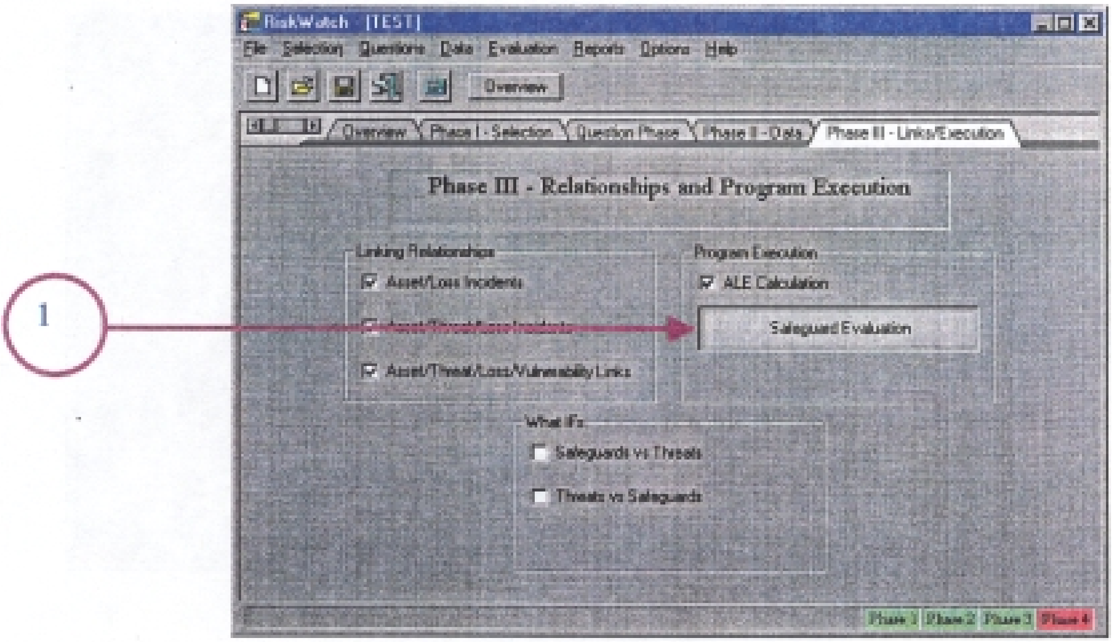
The following list of incidents (threat; loss category; asset category) have no impacted assets. This means that the ALE for these incidents will be 0.

1. Errors, General/All; Direct Loss; Accounts Payable
2. Errors, General/All; Delays/Denials; Accounts Payable
3. Fraud/Embezzlement; Modification; Accounts Payable
4. Inflation; Intangibles; Accounts Payable
5. Errors, General/All; Related Direct Loss; Accounts Payable
6. Data Integrity Loss; Direct Loss; Accounts Payable
7. Currency Fluctuation; Intangibles; Accounts Payable
8. Inflation; Direct Loss; Accounts Payable
9. Data Integrity Loss; Modification; Accounts Payable
10. Inflation; Intangibles; Accounts Receivable
11. Data Integrity Loss; Modification; Accounts Receivable
12. Data Integrity Loss; Direct Loss; Accounts Receivable
13. Fraud/Embezzlement; Modification; Accounts Receivable
14. Errors, General/All; Delays/Denials; Accounts Receivable
15. Errors, General/All; Related Direct Loss; Accounts Receivable

WARNING
Due to an inherent characteristic in the 7.1 version of RiskWatch, multiple incident listings for the same issue may appear. After corrections, subsequent listings of the original incident(s) may reappear.

Safeguard Evaluation

1. Click **Safeguard Evaluation**. Depending on the PC's processor and the review size, the calculation may take several minutes to hours.



Phase III - Relationships and Program Execution

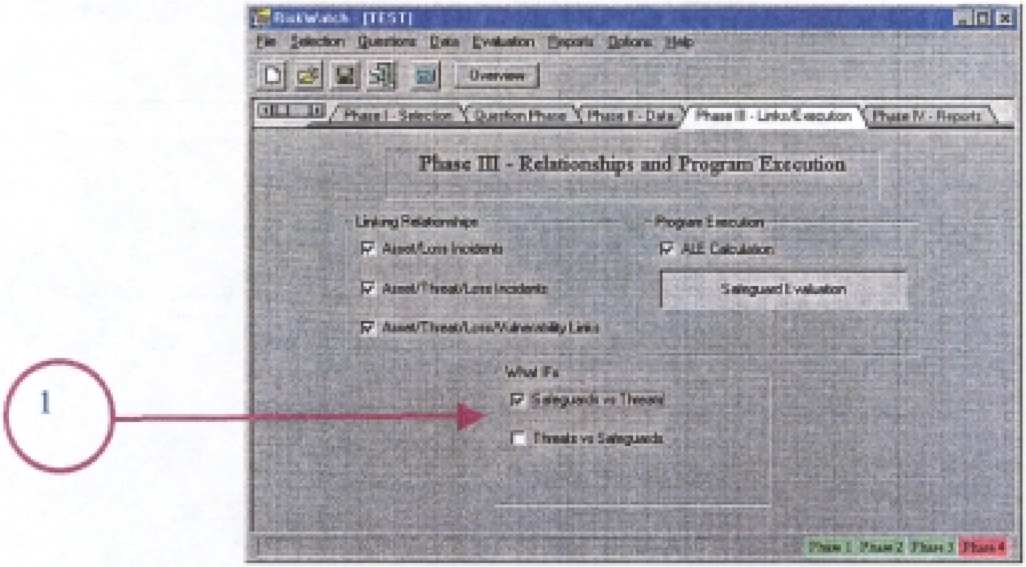
Linking Relationships
☑ Asset/Loss Incidents
☑ Asset/Threat/Loss Incidents
☑ Asset/Threat/Loss/Vulnerability Links

Program Execution
☑ ALE Calculation

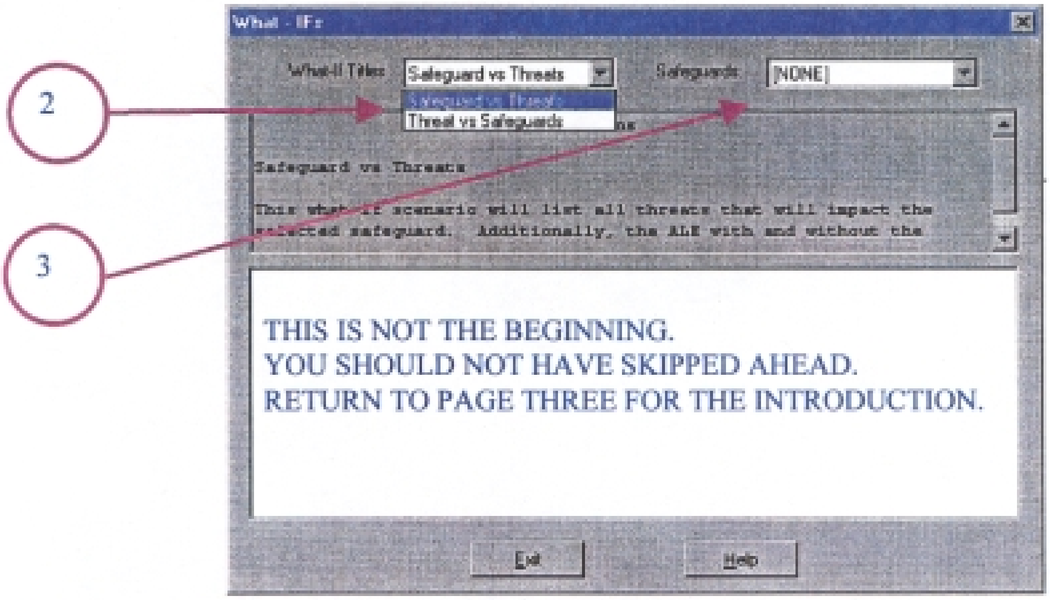
What Ifs
☐ Safeguards vs Threats
☐ Threats vs Safeguards

What Ifs

1. Click the **Safeguards Vs Threats.** The 'What If' dialog box appears.



2. Select **Safeguard vs Threats** or **Threat vs Safeguards**, using the pull down menu.
3. Depending on the selected 'What If' select either a Safeguard or a Threat using the pull down menu. The RiskWatch 'Please Wait….Reading' dialog box appears.



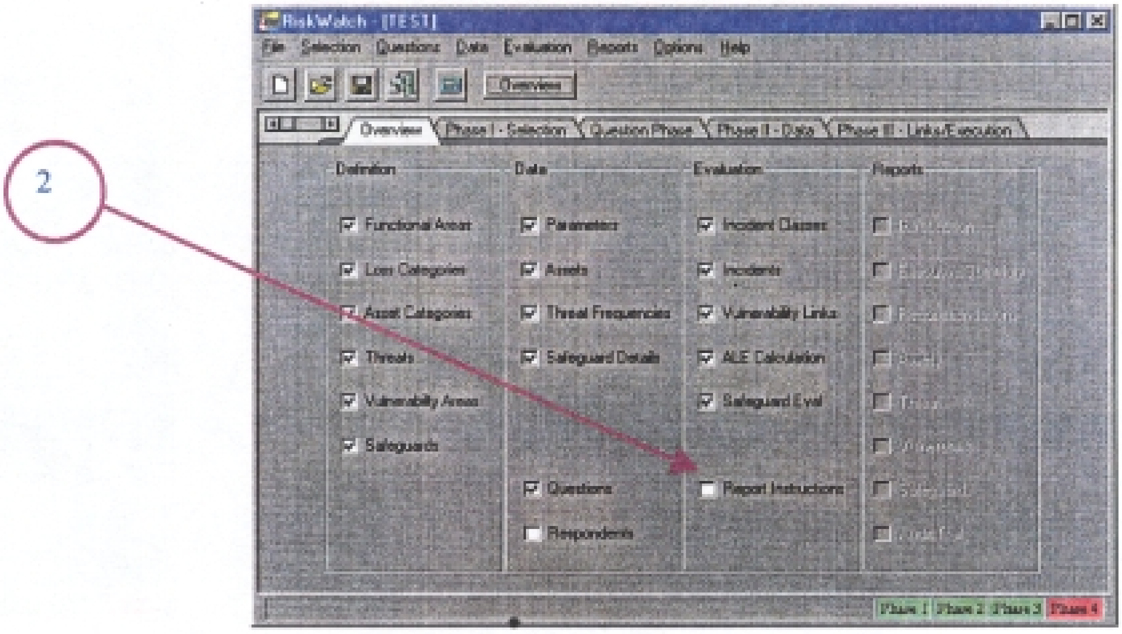
```
Safeguard vs Threats

This what-if scenario will list all threats that will impact the
selected safeguard.  Additionally, the ALE with and without the
```

THIS IS NOT THE BEGINNING.
YOU SHOULD NOT HAVE SKIPPED AHEAD.
RETURN TO PAGE THREE FOR THE INTRODUCTION.

This concludes the tasks for Phase III, Relationships and Program Execution.

Phase IV - Reports

1. If the case is closed, Open it following the steps in Opening An Existing Case on page 40.
2. Select **Report Instruction** in the third column at the bottom. The Report Instructions dialog box appears.



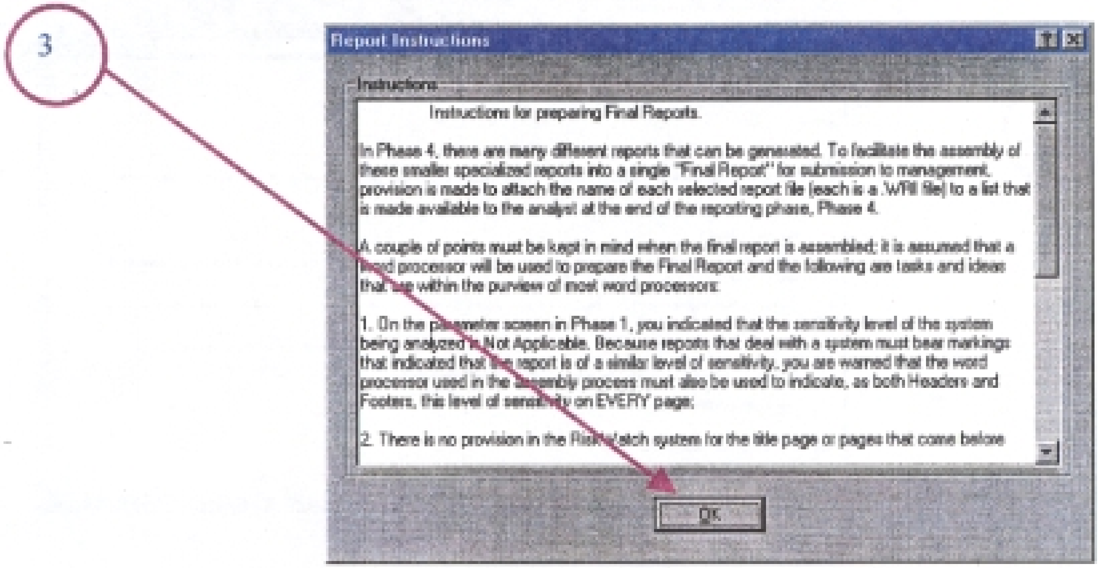
Definition
☑ Functional Areas
☑ Loss Categories
☑ Asset Categories
☑ Threats
☑ Vulnerability Areas
☑ Safeguards

Data
☑ Parameters
☑ Assets
☑ Threat Frequencies
☑ Safeguard Details
☑ Questions
☐ Respondents

Evaluation
☑ Incident Classes
☑ Incidents
☑ Vulnerability Links
☑ ALE Calculation
☑ Safeguard Eval
☐ Report Instructions

Reports
☐ [illegible]
☐ [illegible]
☐ [illegible]
☐ [illegible]
☐ [illegible]
☐ [illegible]
☐ [illegible]
☐ [illegible]

3. Click **OK**, after reading the **Report Instructions**. The Phase IV- Reports tab appears.



Instructions for preparing Final Reports.

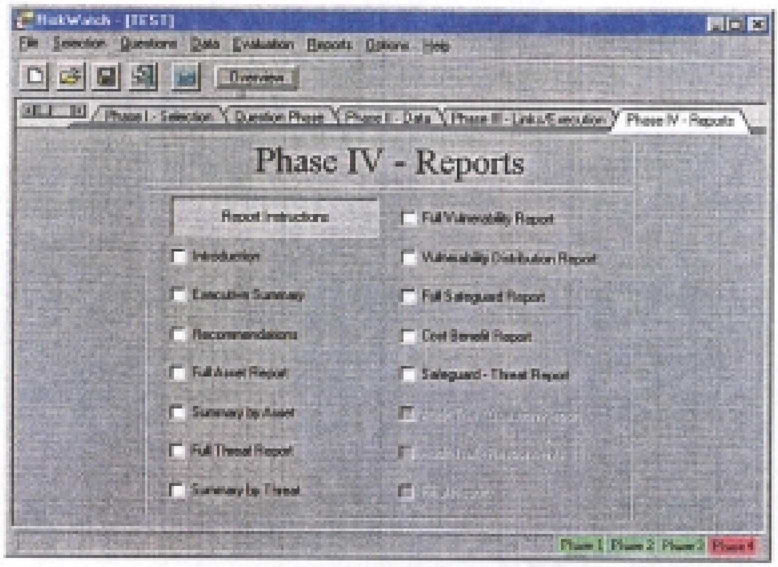
In Phase 4, there are many different reports that can be generated. To facilitate the assembly of these smaller specialized reports into a single "Final Report" for submission to management, provision is made to attach the name of each selected report file (each is a .WRI file) to a list that is made available to the analyst at the end of the reporting phase, Phase 4.

A couple of points must be kept in mind when the final report is assembled; it is assumed that a word processor will be used to prepare the Final Report and the following are tasks and ideas that are within the purview of most word processors:

1. On the parameter screen in Phase 1, you indicated that the sensitivity level of the system being analyzed is Not Applicable. Because reports that deal with a system must bear markings that indicated that the report is of a similar level of sensitivity, you are warned that the word processor used in the assembly process must also be used to indicate, as both Headers and Footers, this level of sensitivity on EVERY page;

2. There is no provision in the RiskWatch system for the title page or pages that come before

4. Click the box for each report to be reviewed. Refer to Section 4 RiskWatch Phase IV - Reports, regarding the contents of each report.


RiskWatch - [TEST]
File Selection Questions Data Evaluation Reports Options Help
Overview
Phase I - Selection
Question Phase
Phase II - Data
Phase III - Links/Execution
Phase IV - Reports
Phase 1 Phase 2 Phase 3 Phase 4

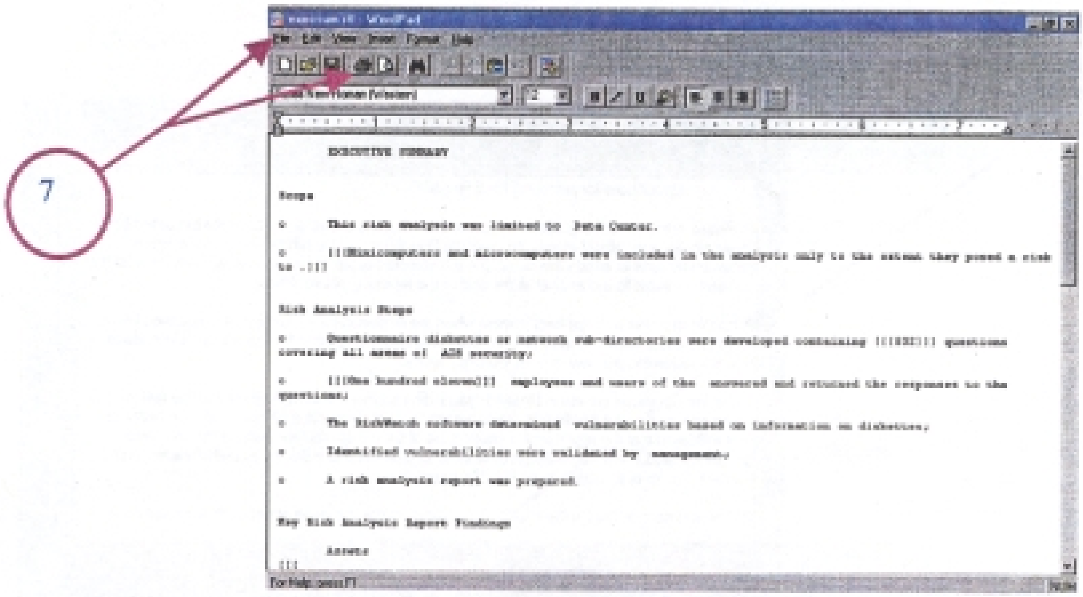
Phase IV - Reports

Report Instructions

☐ Introduction
☐ Executive Summary
☐ Recommendations
☐ Full Asset Report
☐ Summary by Asset
☐ Full Threat Report
☐ Summary by Threat
☐ Full Vulnerability Report
☐ Vulnerability Distribution Report
☐ Full Safeguard Report
☐ Cost Benefit Report
☐ Safeguard - Threat Report

Printing Reports

5. Select any report by clicking once.
6. RiskWatch will launch the default word processor software.
7. The report can be printed by using the print icon button or File, Print commands.



EXECUTIVE SUMMARY

Scope

o This risk analysis was limited to Data Center.

o |||Minicomputers and microcomputers were included in the analysis only to the extent they posed a risk to .|||

Risk Analysis Steps

o Questionnaire diskettes or network sub-directories were developed containing ||||XX||| questions covering all areas of ADS security;

o |||One hundred eleven||| employees and users of the answered and returned the responses to the questions;

o The RiskWatch software determined vulnerabilities based on information on diskettes;

o Identified vulnerabilities were validated by management;

o A risk analysis report was prepared.

Key Risk Analysis Report Findings

Assets

|||

This concludes the tasks for Phase IV, Reports.

Question Phase

Introduction

RiskWatch's Question Phase identifies potential vulnerabilities to the organization or business function. The Question Phase consists of six activities: edit/select questions, establish the answer threshold, identify respondents, prepare question sets, import answers, and produce the question report. This section provides these six suggested steps in detail and provides the step-by-step instructions on how to use RiskWatch in this Phase.

Six Suggested Steps

Overview

The following provides an overview of the six steps used to complete the question phase.

Step 1. Edit/Select Questions
It is most important for beginning RiskWatch users to initially edit, select, and modify questions that come with the RiskWatch software as well as questions developed by other users (e.g., the UINRAP questions). This step eliminates questions not applicable to the organization or agency, and modifies terminology to match that used and understood by perspective respondents in the agency's "local environment".

Step 2. Establish the Answer Threshold
Using the RiskWatch questionnaire program, respondents score the compliance levels of questions involving policy, procedure, security precautions, etc. The respondents use a scale of 0 to 100 percent. The analyst has the responsibility, along with upper management, to establish an acceptable level of compliance for the business function under review. The RiskWatch default is 85 percent.

Step 3. Identify Respondents
In this step, the analyst determines the individuals who have the knowledge and expertise necessary to accurately measure, or score, compliance. RiskWatch requires the analyst to input the respondent's name, to establish a respondent ID, and to select one or more Functional Areas appropriate to the respondent's expertise and knowledge. RiskWatch then produces a set of questions packaged specifically for the respondent's designated Functional Areas.

Step 4. Prepare Question Sets
Preparing question sets allows the analyst to distribute questions to the respondent by disk, E-mail, LAN, etc.

Step 5. Import Answers
Importing answers involves moving the respondents answers into the RiskWatch program by use of disk, e-mail, LAN, etc.

Step 6. Produce the Question Report
In this final step, RiskWatch automatically totals the answers for all chosen respondents and produces a Vulnerability Report.

Step 1: Edit/Select Questions

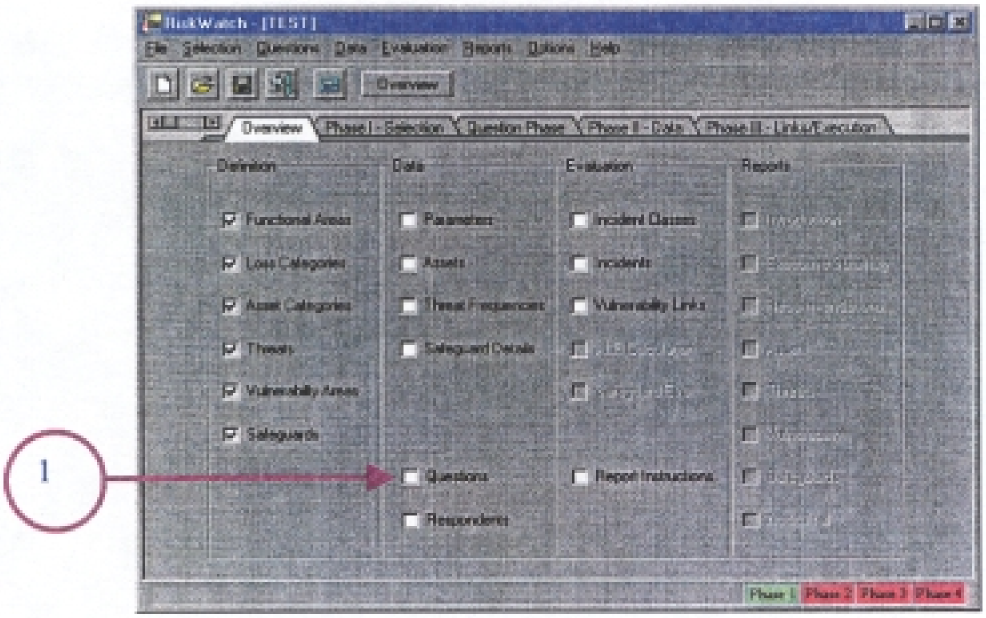
Beginning RiskWatch users need to initially select and edit the RiskWatch questions, as well as questions developed by other users. This step eliminates questions not applicable to the organization or agency and modifies unfamiliar terminology for respondents' better understanding. Be aware that initial selecting and editing questions to fit the agency's needs is quite time consuming. However, by following the step-by-step instructions outlined below, a re-usable UI question database for future risk analyses can be built. (See Building a Re-usable UI Question Database on page 110.).

- Step 1-A: Using the Question Database

If a previously built question database is available, follow the instructions for Using the Question Date Base on page 111 to copy the question database to the new case. If not, follow the instructions for Building a Re-usable UI Question Database on page 110.

- Step 1-B: Selecting Question Categories.

1. Click **Questions.** The Question Phase tab dialog box appears.



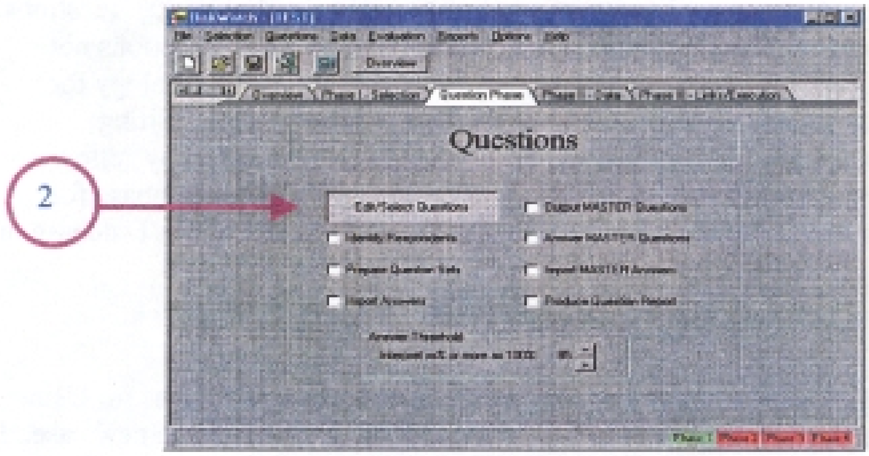
Definition
☑ Functional Areas
☑ Loss Categories
☑ Asset Categories
☑ Threats
☑ Vulnerability Areas
☑ Safeguards

Data
☐ Parameters
☐ Assets
☐ Threat Frequencies
☐ Safeguard Details
☐ Questions
☐ Respondents

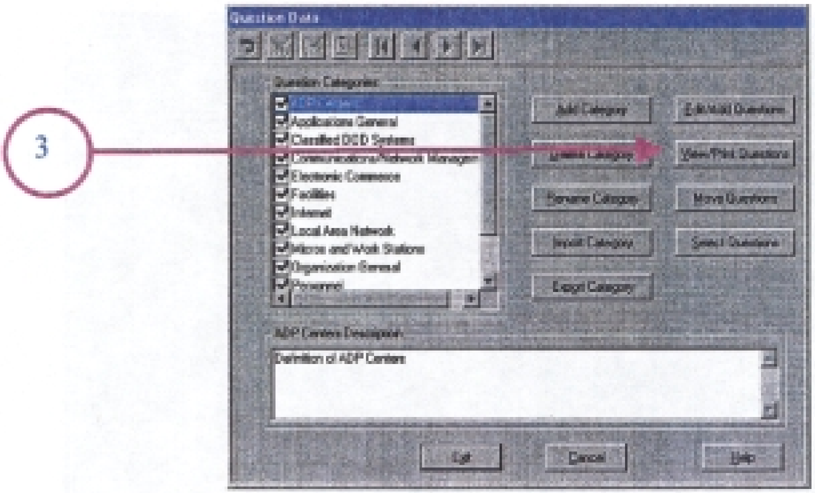
Evaluation
☐ Incident Classes
☐ Incidents
☐ Vulnerability Links
☐ Report Instructions

Reports

2. Click **Edit/Select**. The Question Data dialog box appears.



3. Select **View/Print Questions**

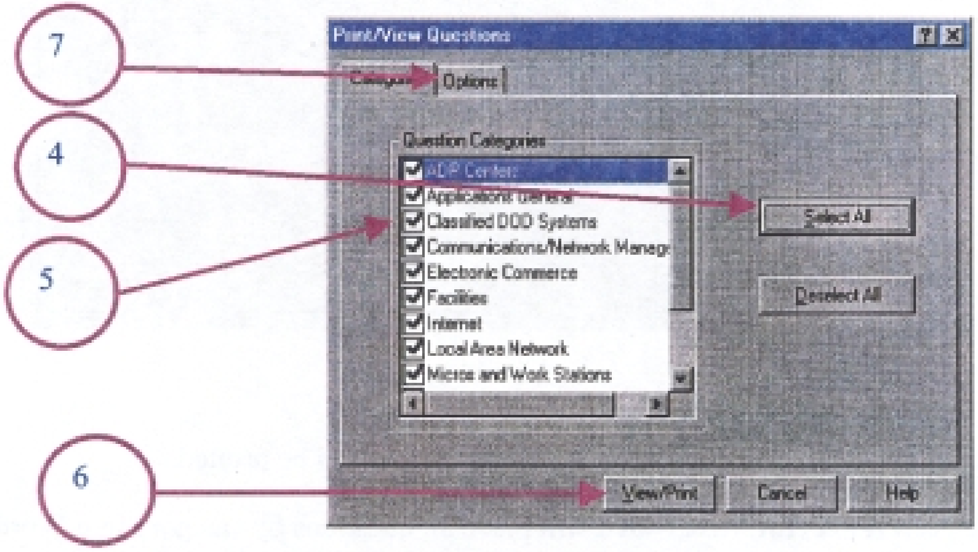


4. Click once on the **Select All** button.

5. Place cursor over the box to the left of Classified DOD Systems and click once to deselect this Question Category.

6. If all the information related to each question is chosen, Click **Print/View** and go to step 11. If not, continue to step 7.

7. Click **Options tab**. The Print/View Question dialog appears.

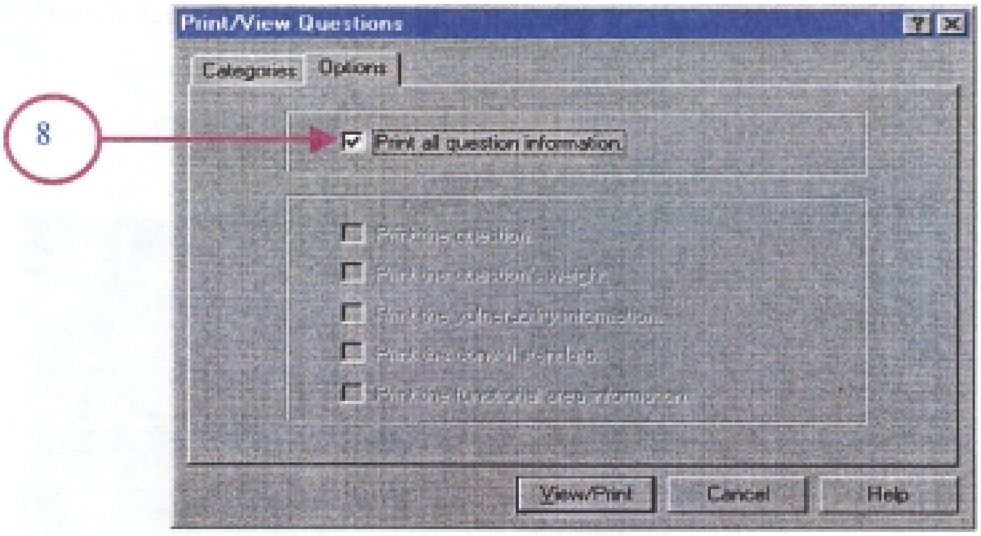


Question Categories

☑ ADP Centers
☑ Applications General
☑ Classified DOD Systems
☑ Communications/Network Manage
☑ Electronic Commerce
☑ Facilities
☑ Internet
☑ Local Area Network
☑ Micros and Work Stations

- Step 1-C: Print out Questions.

8. Click once on the **Print all question information** box to deselect. All print options will now be available.

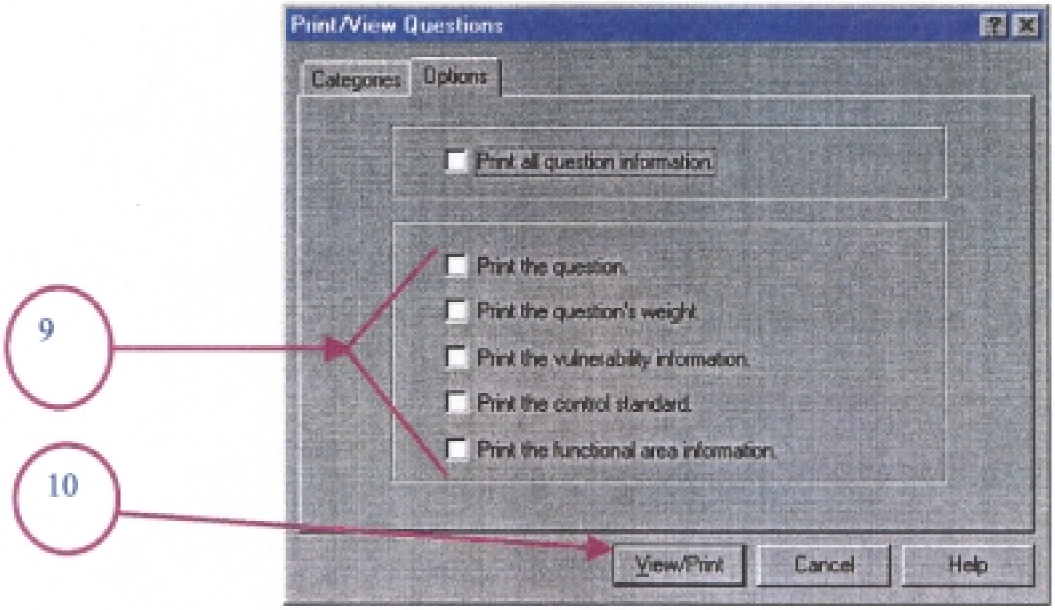


☑ Print all question information.

□ Print the question.
□ Print the question's weight.
□ Print the vulnerability information.
□ Print the control standard.
□ Print the functional area information.

9. Click over the box to the left of each option needs to be printed.

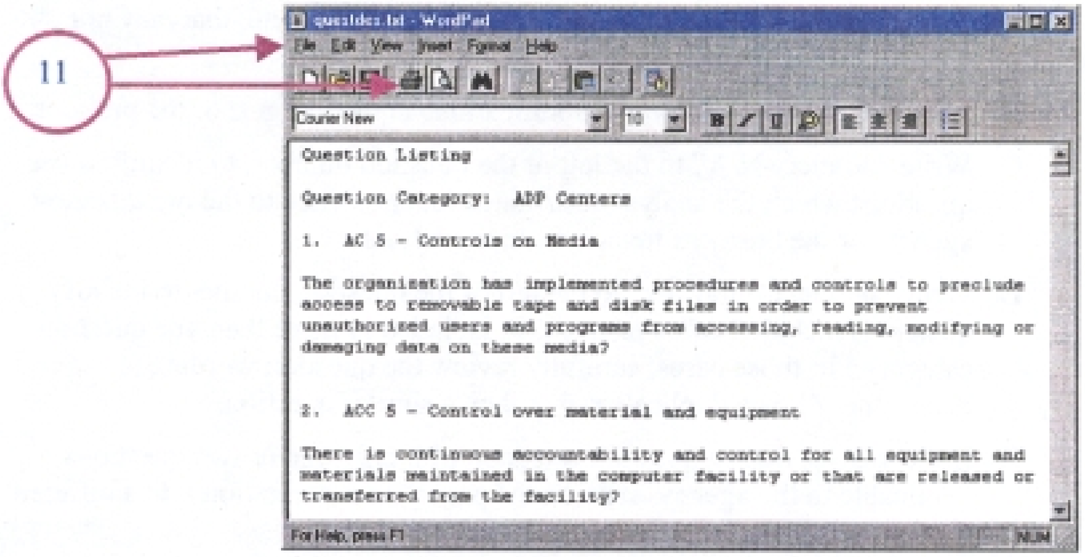
10. Select **View/Print**. RiskWatch will place all questions by category into Word or WordPad.



□ Print all question information.

□ Print the question.
□ Print the question's weight.
□ Print the vulnerability information.
□ Print the control standard.
□ Print the functional area information.

11. Select **File, Print** or the **print icon** button. All the questions in RiskWatch (except DOD Systems) as well as the UINRAP questions will be printed (more than 1300 Questions total).



```
Question Listing

Question Category:  ADP Centers

1.   AC 5 - Controls on Media

The organization has implemented procedures and controls to preclude
access to removable tape and disk files in order to prevent
unauthorized users and programs from accessing, reading, modifying or
damaging data on these media?


2.   ACC 5 - Control over material and equipment

There is continuous accountability and control for all equipment and
materials maintained in the computer facility or that are released or
transferred from the facility?
```

12. If in later cases the analyst wishes to print the question again, the file needs to be saved with a different name. Click **File, Save As** and name the file.

13. Click **File, Close** to exit.

- Step 1-D: Using the Printout to Edit / Modify Questions

14. Edit the questions by marking with pencil or pen using the following suggestions:

    A. Circle questionable terminology, acronyms, phrases, etc. that may not understood in the organization or business function.

    B. Write-in the necessary word modifications in the margins of the printout.

    C. Write "deselect-N/A" to the left of the question number, to identify those questions which the analyst determined inappropriate to the organization, agency, or the business function under analysis.

    D. Write "deselect-duplicate" to the left of the question number to identify questions included twice or more, or included in more than one question category. In those cases, carefully review the question wording to determine if it is a duplicate rather than a similar question.

    E. If the analyst finds a question category with only one or two questions applicable to the agency write on the page: "Move question # to a different question category, and then deselect this category."

    F. If the analyst determines that the entire question category does not apply to the agency, write on the top of the page, "Deselect the entire question category".

After the analyst penciled in the modifications and identified the questions to be deleted or moved, then make the changes in RiskWatch.

- Step 1-E: Edit/Modify Questions in the RiskWatch

15. In RiskWatch, modify the wording, acronyms, phrases, etc., using the annotated printout and following the "Modify Individual Questions" step-by-step procedures on page 131.

16. In RiskWatch, deselect individual questions, which the analyst marked as not applicable or duplicative, using the annotated printout and following the "Select Individual Question" step-by-step procedures on page 134.

17. In RiskWatch, move questions the analyst marked on the annotated printout by following the "Moving Individual Question" step-by-step procedures on page 141. After moving the questions, deselect the category following the "De-select Question Category" step-by-step procedures on page 112.

18. In RiskWatch, deselect entire question categories not applicable to the agency or analysis by using the annotated printout and following the "De-select Question Category" step-by-step procedures on page 112.

Step 2: Establish the Answer Threshold

With the RiskWatch questionnaire program, respondents are asked to score levels of compliance to questions involving policy, procedure, security precautions, etc., on a scale of 0 to 100. A zero (0) score indicates no compliance, in the respondent's opinion. A one hundred (100) score indicates total compliance. Any score between 0 and 100 indicates varying degrees of partial compliance as interpreted by the respondent for a given question.

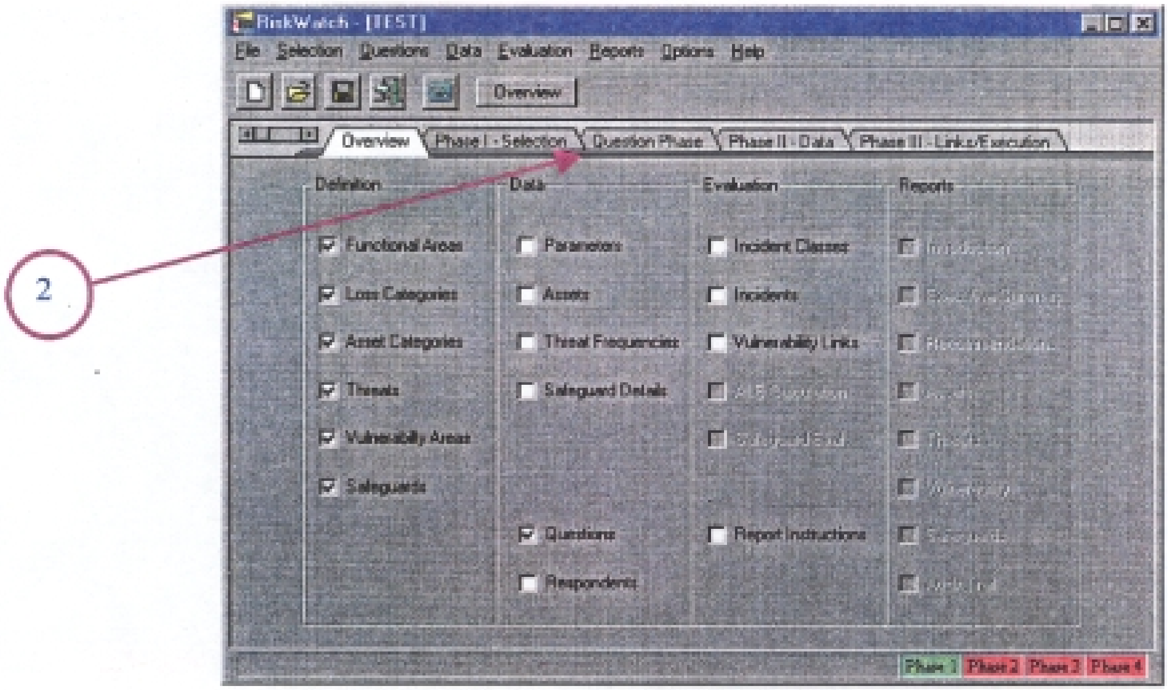
If the answer threshold is 85 (the default value), RiskWatch interprets "scores" that equal or exceed the threshold of 85 as compliant. Therefore, those vulnerability statements do not appear on the Vulnerability Report. Likewise, RiskWatch interprets respondent "scores" that fall below the default "answer threshold" of as non-compliant and includes them in the Vulnerability Report.

RiskWatch allows experienced users the option to change the "answer threshold" from 85 to any other number between 0 and 100.

TIP
It is recommended that less experienced users should not change the RiskWatch default value of 85.

Step by step instructions:

1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select **Question Phase** tab.



Definition

- ☑ Functional Areas
- ☑ Loss Categories
- ☑ Asset Categories
- ☑ Threats
- ☑ Vulnerability Areas
- ☑ Safeguards

Data

- □ Parameters
- □ Assets
- □ Threat Frequencies
- □ Safeguard Details
- ☑ Questions
- □ Respondents

Evaluation

- □ Incident Classes
- □ Incidents
- □ Vulnerability Links
- □ [illegible]
- □ [illegible]
- □ Report Instructions

Reports

- □ [illegible]
- □ [illegible]
- □ [illegible]
- □ [illegible]
- □ [illegible]
- □ [illegible]
- □ [illegible]
- □ [illegible]

3. Locate the Answer Threshold area at the bottom of the Question Phase tab.

To Raise Threshold

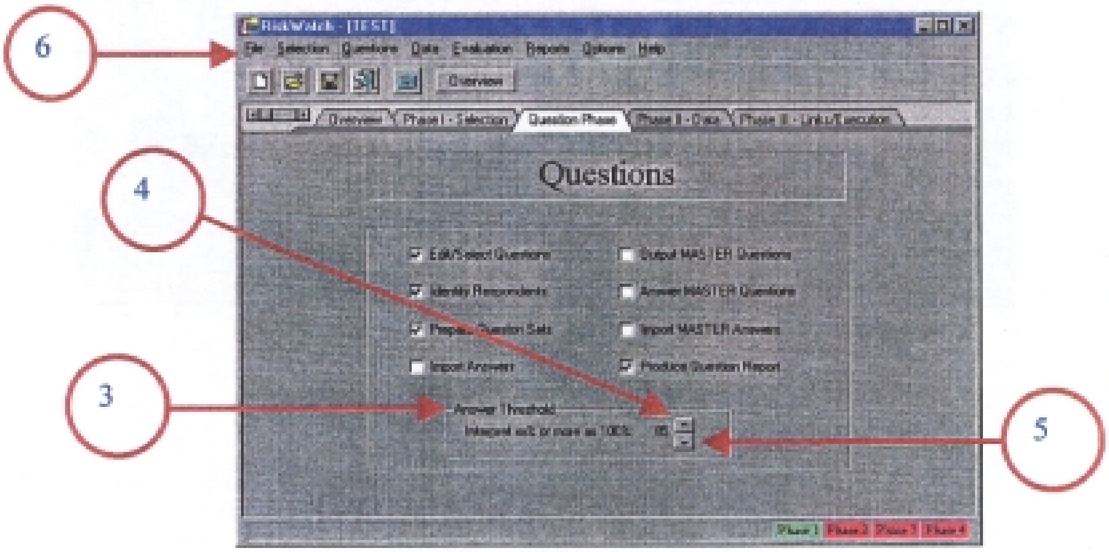
4. Raise the threshold by placing the cursor on the up triangle and click until the desire percentage is reached. Each click increases the number by one (1).

To Lower Threshold

5. Lower the threshold by placing the cursor on the down triangle and clicking until the desire percentage is reached. Each click decreases the number by one (1).

6. **File, Save**.

Thus, the threshold changes from the 85 "default value" to the **Answer Threshold** value appropriate to the analysis.



☑ Edit/Select Questions
☑ Identify Respondents
☑ Prepare Question Sets
☐ Import Answers
☐ Output MASTER Questions
☐ Answer MASTER Questions
☐ Import MASTER Answers
☑ Produce Question Report

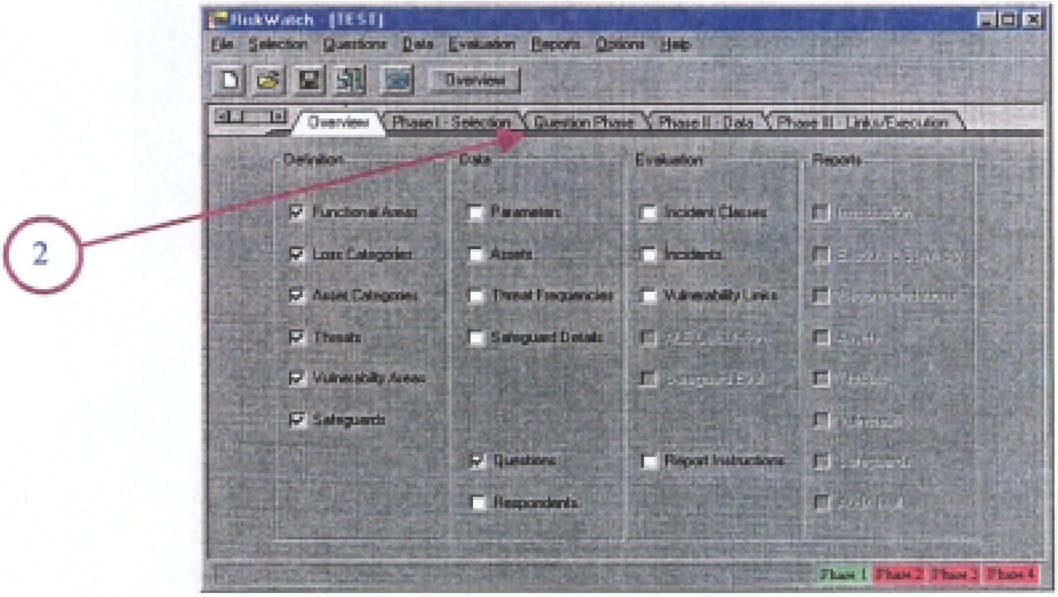
Answer Threshold
Interpret xx% or more as 100%: 85

Step 3: Identify Respondents

Using the data collected in Section 4, the analyst identifies the appropriate respondents for the risk analysis. The analyst then inputs the names, IDs, and Functional Areas for each respondent. Using this information, RiskWatch develops question sets tailored to each respondent.

Step by step instructions: Identifying Respondents:

1. Open RiskWatch following Opening An Existing Case on page 40.
2. Select **Question Phase tab**.


2
RiskWatch - [TEST]
File Selection Questions Data Evaluation Reports Options Help
Overview
Overview
Phase I - Selection
Question Phase
Phase II - Data
Phase III - Links/Execution
Phase 1 Phase 2 Phase 3 Phase 4

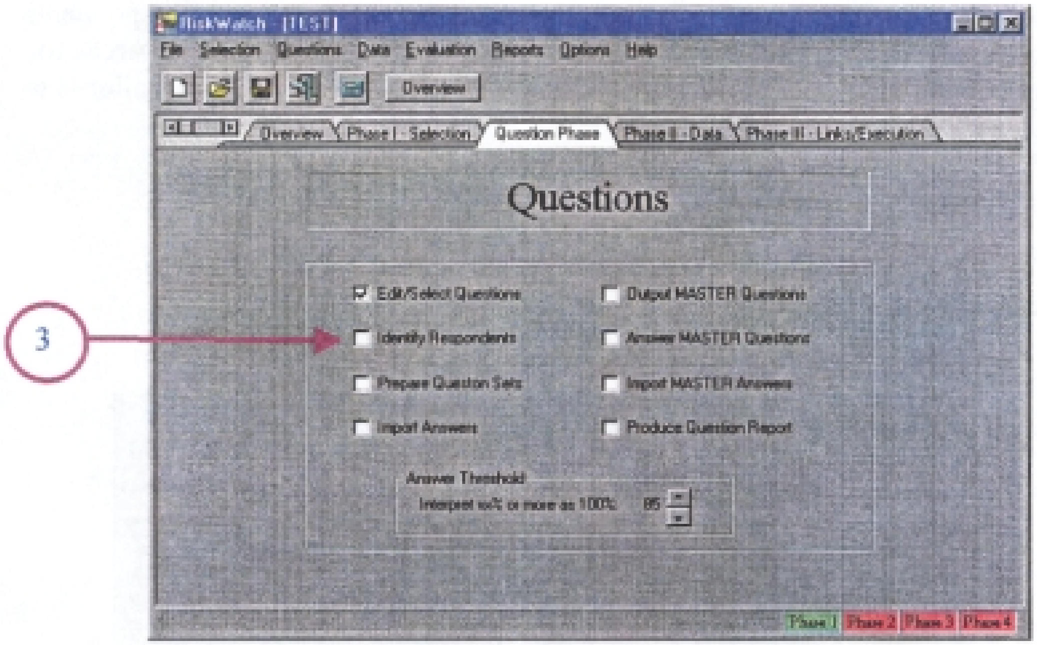
Definition
- ☑ Functional Areas
- ☑ Loss Categories
- ☑ Asset Categories
- ☑ Threats
- ☑ Vulnerability Areas
- ☑ Safeguards

Data
- □ Parameters
- □ Assets
- □ Threat Frequencies
- □ Safeguard Details
- ☑ Questions
- □ Respondents

Evaluation
- □ Incident Classes
- □ Incidents
- □ Vulnerability Links
- □ Report Instructions

Reports

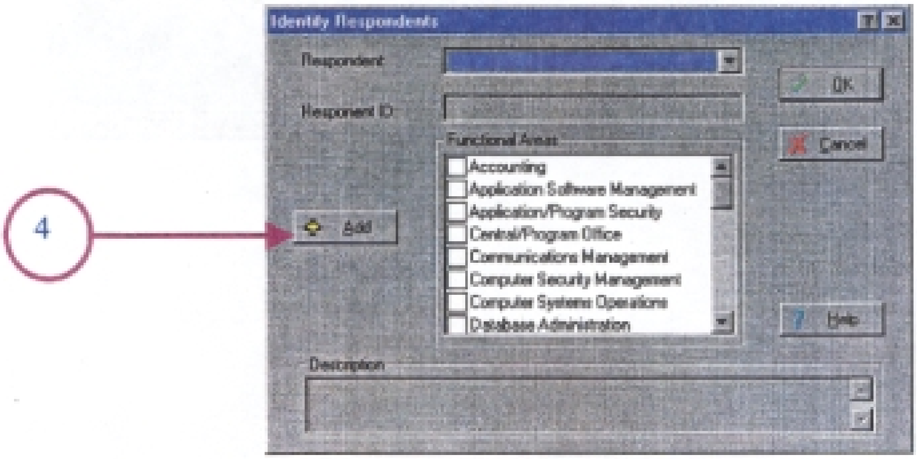
3. Select **Identify Respondents**, the Identify Respondents dialog box appears.



☑ Edit/Select Questions
□ Identify Respondents
□ Prepare Question Sets
□ Import Answers
□ Output MASTER Questions
□ Answer MASTER Questions
□ Import MASTER Answers
□ Produce Question Report

Answer Threshold
Interpret xx% or more as 100%: 85

4. Select **Add**. The Add Respondent dialog box appears.

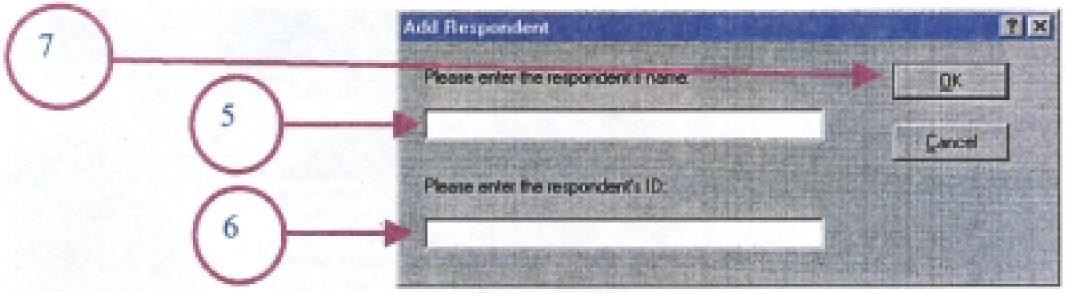


□ Accounting
□ Application Software Management
□ Application/Program Security
□ Central/Program Office
□ Communications Management
□ Computer Security Management
□ Computer Systems Operations
□ Database Administration

5. Type in the respondent's name.

6. Move the cursor to the Respondents ID box and type in an ID. (Note: Keep the ID simple and easy to remember or associate with the respondent.)

7. Select **O.K.** The Identify Respondents dialog box appears.

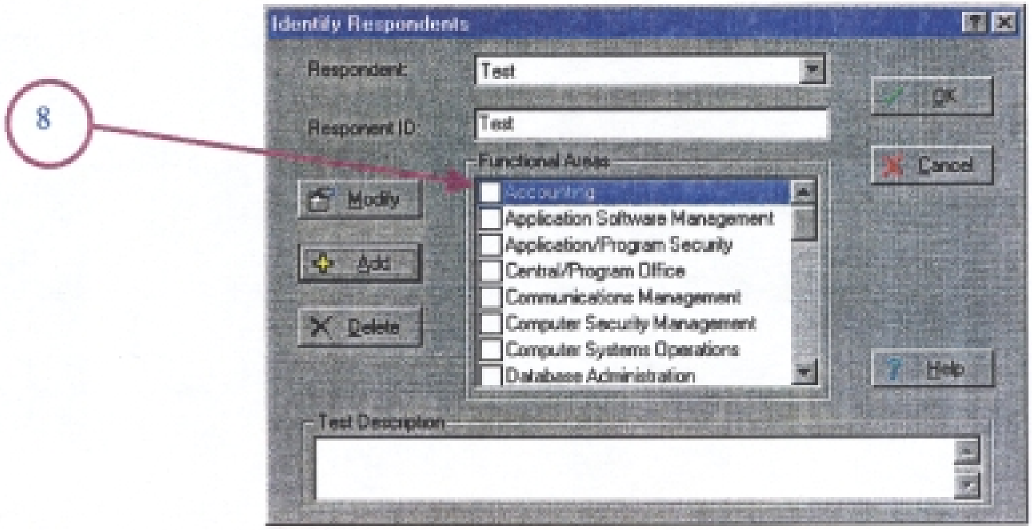


Add Respondent

Please enter the respondent's name:

Please enter the respondent's ID:

8. Click the box to the left of the respondent's **Functional Areas**. If no **Functional Areas** are appropriate, add **Functional Areas** by following the instructions in Adding a Functional Area on page 43.



Identify Respondents

Respondent: Test

Responent ID: Test

Functional Areas

□ Accounting
□ Application Software Management
□ Application/Program Security
□ Central/Program Office
□ Communications Management
□ Computer Security Management
□ Computer Systems Operations
□ Database Administration

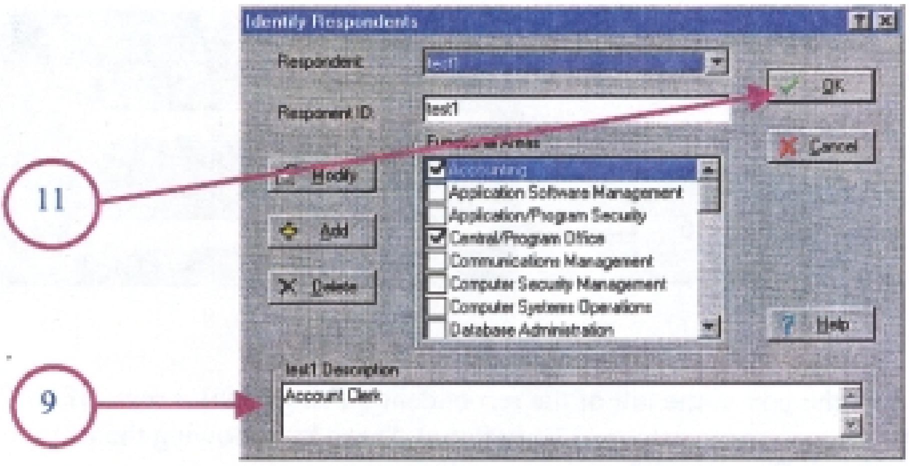
Test Description

WARNING
If the analyst have numerous respondents, **Save** after every 10-12 entries. Go to step 11 and Save.

9. OPTIONAL: Enter a description of the respondent in the box across the bottom of the Identify Respondents dialog box.

10. Repeat Steps 4 to 8 as needed. When done, continue to Step 11.

11. Select **O.K.**, the Question Phase screen re-appears.



Respondent: test1

Respondent ID: test1

Functional Areas

☑ Accounting
☐ Application Software Management
☐ Application/Program Security
☑ Central/Program Office
☐ Communications Management
☐ Computer Security Management
☐ Computer Systems Operations
☐ Database Administration

test1 Description

Account Clerk

12. Save

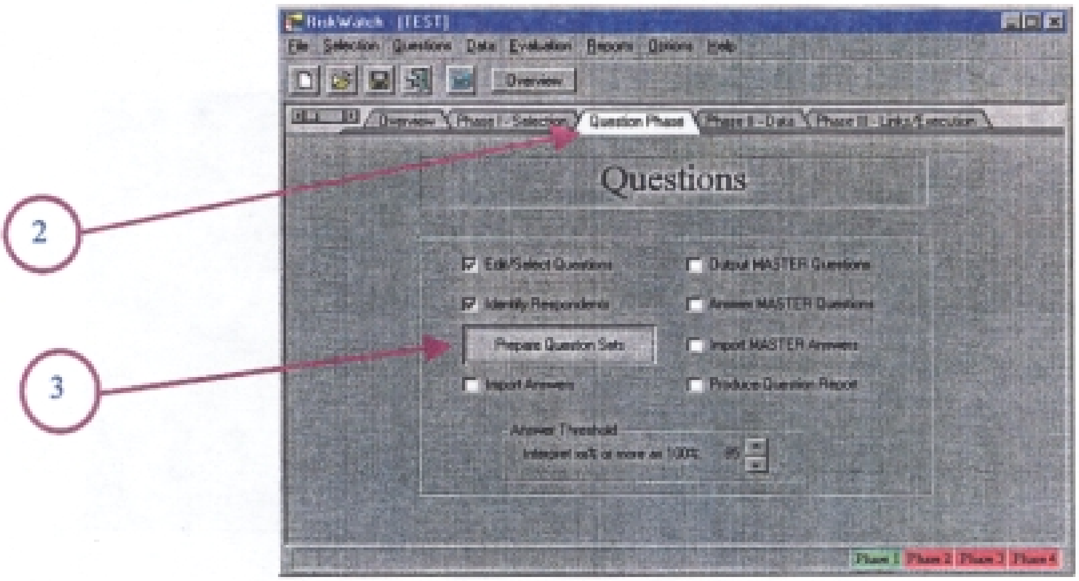
Step 4: Prepare Question Sets

Preparing question sets allows the analyst to distribute questions to the respondent in various ways: paper copy, diskette, e-mail attachment, LAN shared drives, etc.

For this exercise, we create questionnaires on diskettes. The respondents receive the diskettes along with instruction on how to access the diskette and answer the questions. The respondent returns the diskette to the analyst after answering the questions.

Step by step instructions: Preparing Question Sets

1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select **Question Phase tab**
3. Select **Prepare Question Sets**, the Prepare Question Sets dialog box appears.



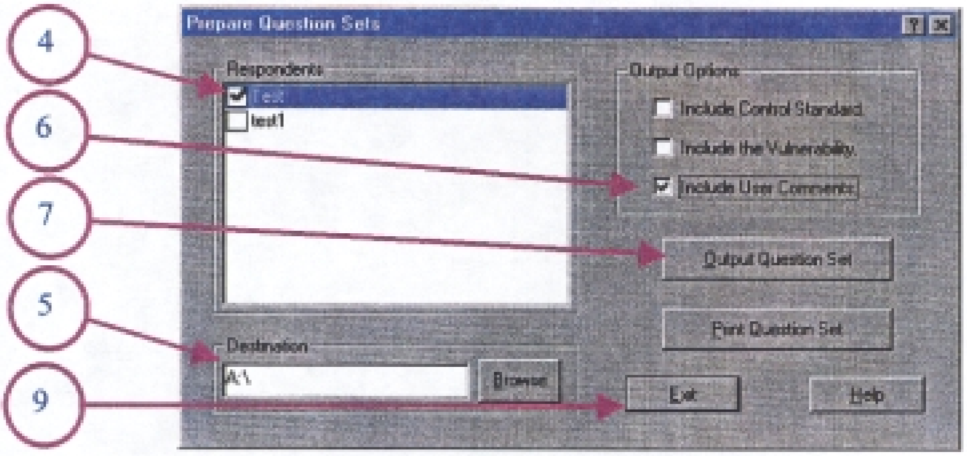
☑ Edit/Select Questions
☑ Identify Respondents
□ Import Answers
□ Output MASTER Questions
□ Answer MASTER Questions
□ Import MASTER Answers
□ Produce Question Report

Interpret xx% or more as 100%: 95

4. **Click** the box next to the respondent's name, to highlight the respondent.
5. Move the cursor to the **Destination** box. Type in "**A:\**" as shown below.
6. Move the cursor to the **Output Options** section of the screen. If the analyst wants comments from the respondents, select **Include User Comments**.
7. Select **Output Question Set**. (Note: This process will take several minutes depending on the PC capabilities.)

> TIP
> Label diskettes with the respondent's name and ID. Secure the diskettes to ensure the ID is not compromised.

8. Repeat Steps 4 to 7 until each respondent's diskette is created.
9. When finished creating the diskettes, select **Exit**. RiskWatch returns to the Question Phase tab.



Prepare Question Sets

Respondents
☑ Test
☐ test1

Output Options
☐ Include Control Standard
☐ Include the Vulnerability
☑ Include User Comments

Destination
A:\

10. Distribute the diskettes to the respective respondents, along with the instruction on how to answer the questions. Refer to the next page for Questionnaire Program Instructions.

Questionnaire Program Instructions

THIS IS NOT A TEST. THERE IS NO RIGHT OR WRONG ANSWER.

ALL INDIVIDUAL RESPONSES WILL BE KEPT CONFIDENTIAL

The diskette provided to you contains policy statements, procedural statements, statements concerning security precautions, etc. The program will ask you to assess levels of compliance by scoring each statement on a scale of 0 to 100. How you score each statement should be based on your judgement, experience, opinion, etc.

All individual responses will be kept confidential. The responses you make will be imported directly into a PC where the answers from all respondents will be automatically compiled.

How to determine your numeric response:

- A score of 100 indicates that, in your judgement, there is 100% compliance with the statement.
- A score of 60 would indicate that you feel compliance to the statement occurs 60% of the time.
- A score of 0 would indicate total non-compliance.
- If you do not know how to gauge a particular statement, click the **I don't know** circle.
- In your assessment, if the statement does not apply, click the **Does not apply** circle.

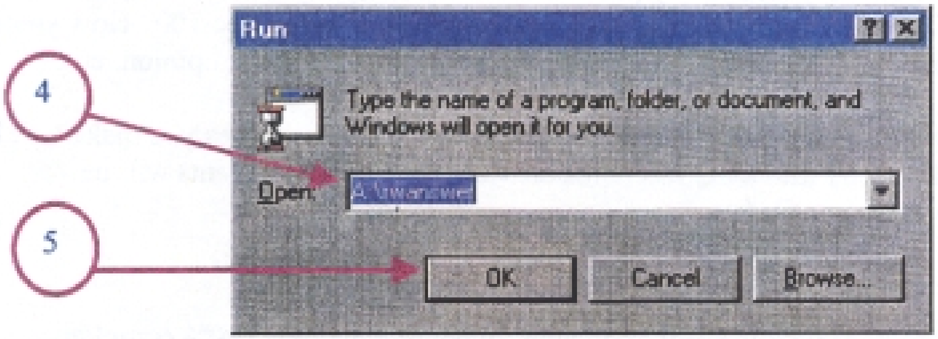
Each question also provides you the opportunity to include comments about the statement or your response. Use whenever you feel it is appropriate.

If you have any questions, call (contact name) at (contact phone number(s)). Please complete the questionnaire by (due date) and return it in the pre-addressed envelope provided.

- *Thank you for your participation in this risk analysis.*

Starting the Questionnaire

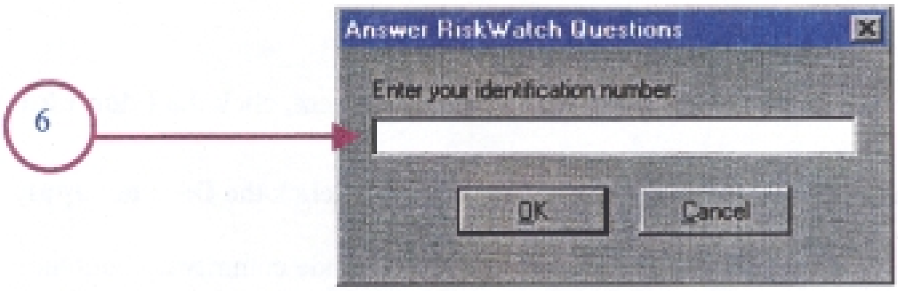
1. Place the diskette in the 'A' drive.
2. Using Windows 95, Click **Start, Run**.
3. Using Windows 3.X, in program manager, select **File** then select **Run**.
4. Type "**a:\rwanswer**"in the dialog box.
5. Click **O.K.** button.



Type the name of a program, folder, or document, and Windows will open it for you.

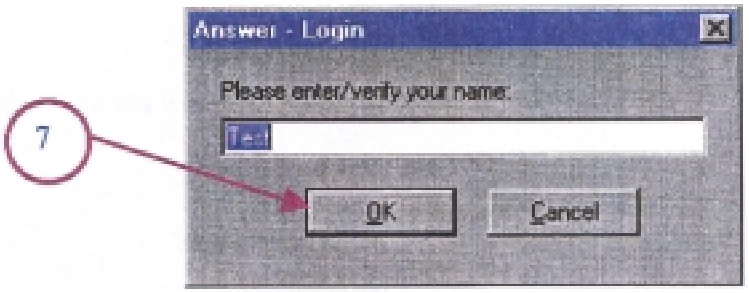
Open: A:\rwanswer

6. Type in your ID, select **O.K.**



Enter your identification number:

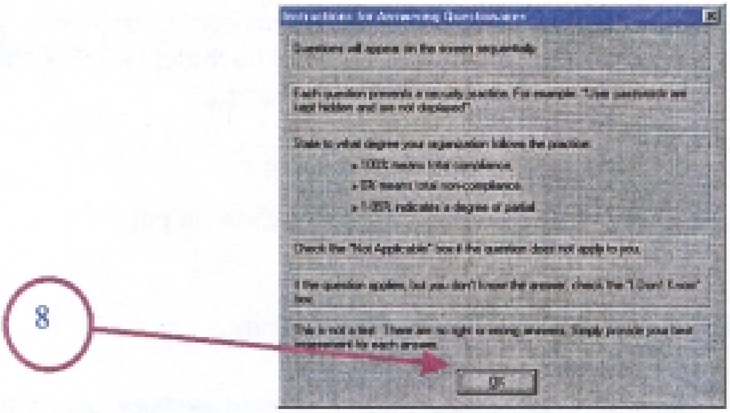
7. Verify your identity, then select **O.K.**



Please enter/verify your name:

Test

8. Read the Instructions for Answering Questions, then select **OK**.



Instructions for Answering Questionnaires

Questions will appear on the screen sequentially.

Each question presents a security practice. For example: "User passwords are kept hidden and are not displayed"

State to what degree your organization follows the practice:

- 100% means total compliance
- 0% means total non-compliance
- 1-99% indicates a degree of partial

Check the "Not Applicable" box if the question does not apply to you.

If the question applies, but you don't know the answer, check the "I Don't Know" box.

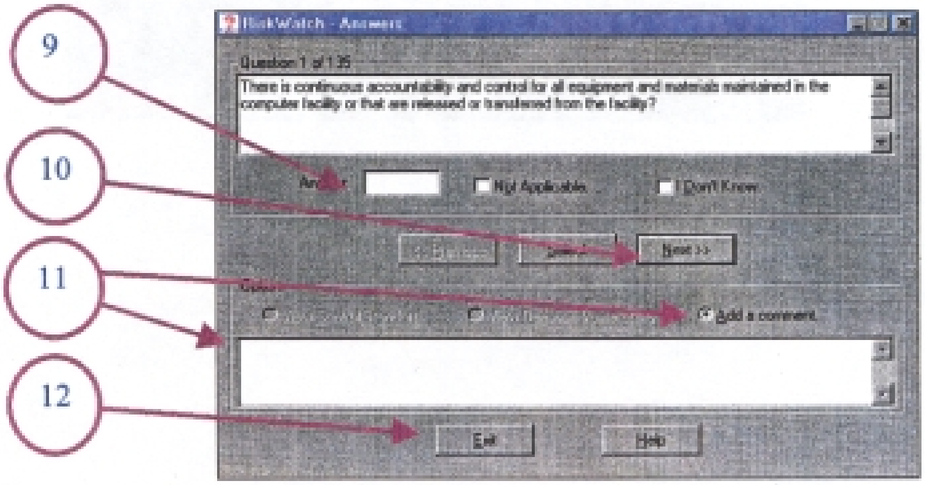
This is not a test. There are no right or wrong answers. Simply provide your best assessment for each answer.

9. Score ALL the statements on a scale of 0-100.

10. Once the score is entered, select **Next**. The next statement appears. Continue until all the questions are answered.

11. To add comments or clarifying statements, click the **Add A Comment** circle and move the cursor to the space designated for comments, and **type** the comments.

12. After all the questions have been answered, click on the **Exit** button. Return the diskette to the individual designated on the instructions.



RiskWatch - Answers

Question 1 of 135

There is continuous accountability and control for all equipment and materials maintained in the computer facility or that are released or transferred from the facility?

Answer:

□ Not Applicable □ I Don't Know

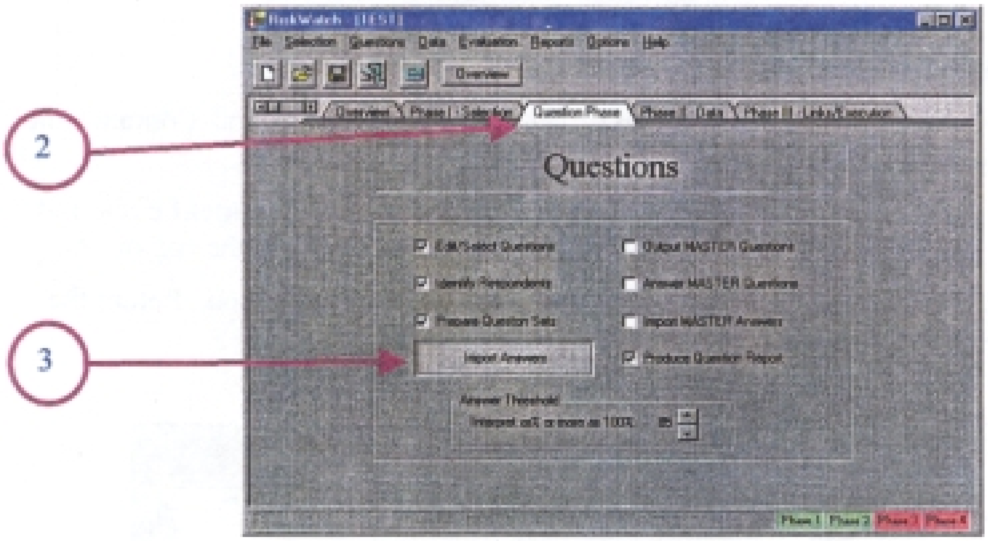
○ [illegible] ○ [illegible] ● Add a comment

Step 5: Import Answers

Importing answers involves moving the respondent's answers into the RiskWatch program in various ways: paper copy, diskette, e-mail attachments, LAN shared drive, etc. In the following instructions, we import from a diskette.

Step by step instructions: Import respondent answers

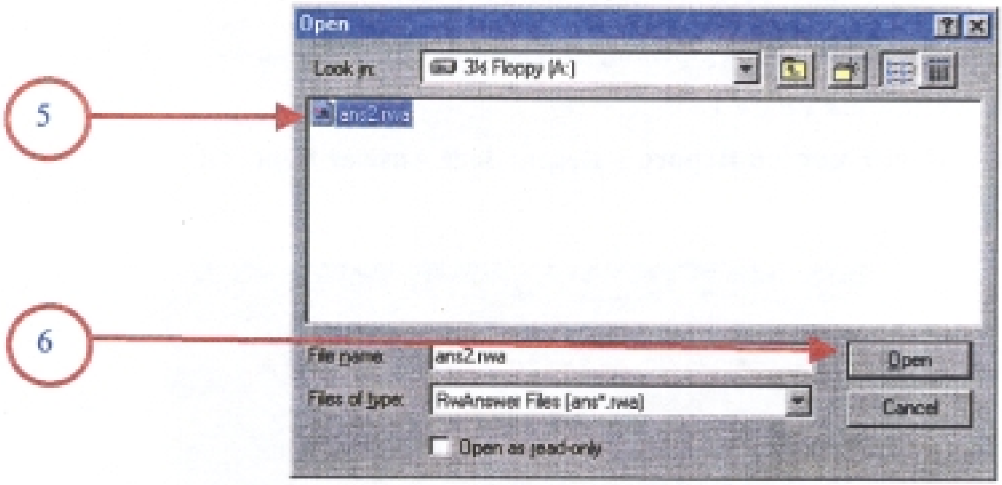
1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select the **Question Phase** Tab.
3. Select **Import Answers**, the **Open** dialog box appears.



☑ Edit/Select Questions
☑ Identify Respondents
☑ Prepare Question Sets
□ Output MASTER Questions
□ Answer MASTER Questions
□ Import MASTER Answers
☑ Produce Question Report

Answer Threshold
Interpret xx% or more as 100% 85

4. Place the disk in Drive 'A'
5. Locate and highlight the "ans*.rwa" file on the diskette in drive A.
6. Select **Open**. The screen flashes quickly as RiskWatch imports the respondent's answers. RiskWatch returns to the Question Phase dialog box.



Look in: 3½ Floppy (A:)

ans2.rwa

File name: ans2.rwa

Files of type: RwAnswer Files (ans*.rwa)

□ Open as read-only

7. Repeat steps 3 to 6 for each respondent.

WARNING
If numerous respondents, Save after every 10 -12 imports.

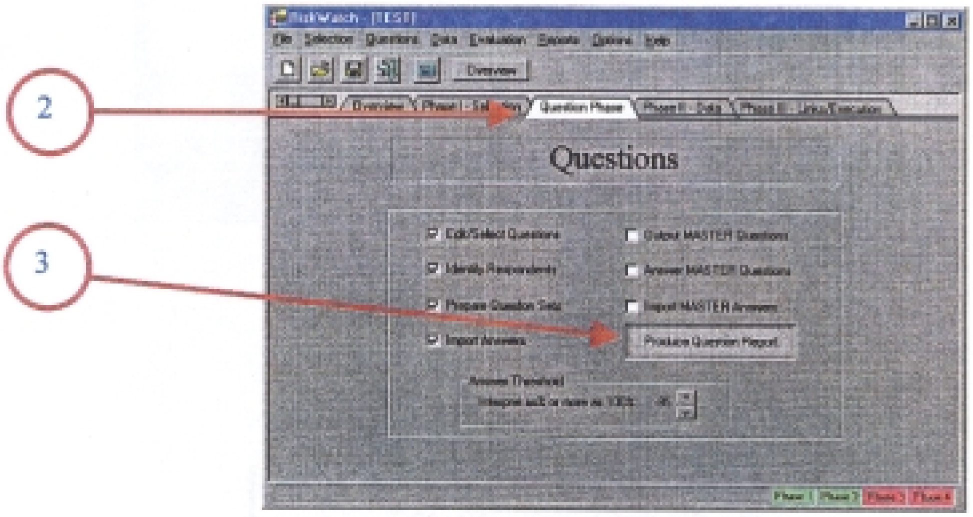
8. **File, Save.**

Step 6: Produce the Question Report

In this final step, the RiskWatch program automatically totals the answers from all chosen respondents and a Vulnerability Report is produced.

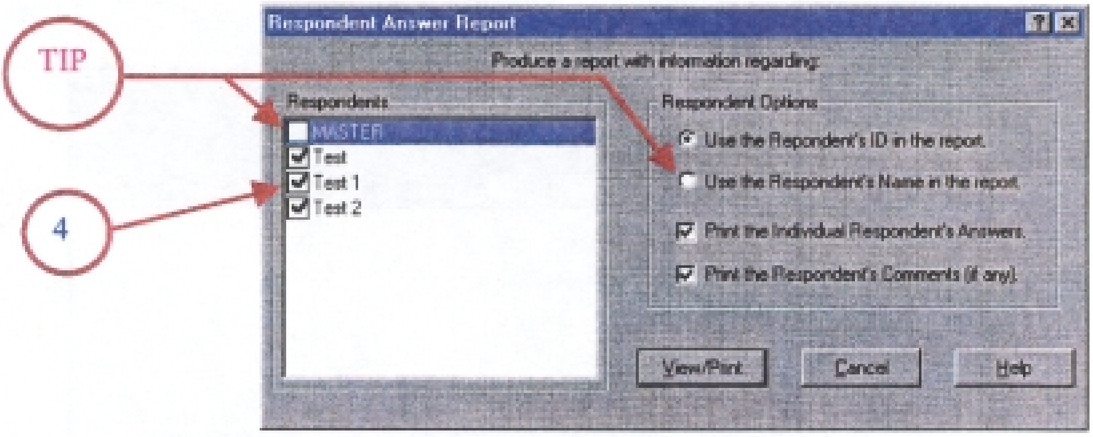
Step by step instructions: Produce the Question Report

1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select the **Question Phase** Tab.
3. Select **Produce Question Report**, a **Respondent Answer Report** dialog box appears.



☑ Edit/Select Questions
☑ Identify Respondents
☑ Prepare Question Sets
☑ Import Answers
□ Output MASTER Questions
□ Answer MASTER Questions
□ Import MASTER Answers

4. For each respondent that the analyst wants to include in the report, **click** the box to the left of the respondent's name.



Respondent Answer Report

Produce a report with information regarding:

Respondents

□ MASTER
☑ Test
☑ Test 1
☑ Test 2

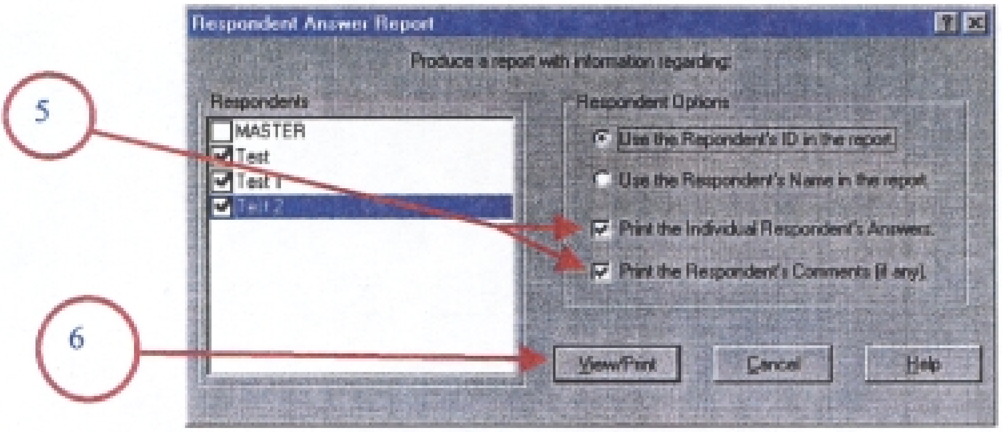
Respondent Options

● Use the Respondent's ID in the report.
○ Use the Respondent's Name in the report.
☑ Print the Individual Respondent's Answers.
☑ Print the Respondent's Comments (if any).

TIP
Deselect "Master", as using "Master" can confuse inexperienced users. In the Respondent Options box, we recommend deselecting the "Use the Respondent's Name in the report" to maintain respondent confidentiality.

5. Select all the options in the Respondent Options block.

6. Select **View/Print**, A Generating Query dialog box appears.



Respondent Answer Report

Produce a report with information regarding:

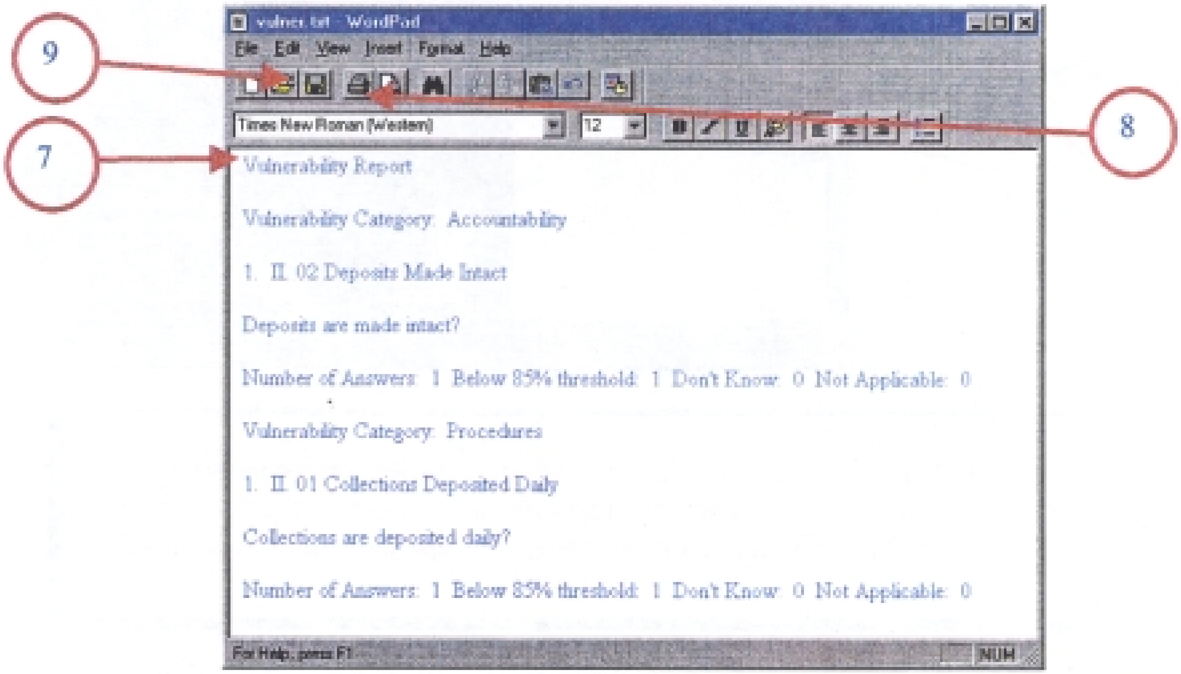
Respondents

□ MASTER
☑ Test
☑ Test 1
☑ Test 2

Respondent Options

● Use the Respondent's ID in the report.
○ Use the Respondent's Name in the report.
☑ Print the Individual Respondent's Answers.
☑ Print the Respondent's Comments (if any).

7. RiskWatch opens Word or WordPad to display the Vulnerability Report.
8. Print the report, click the **Printer icon button** or **File, Print**.
9. Save the report, click the **Diskette icon button** or **File, Save**.



Vulnerability Report

Vulnerability Category: Accountability

1. II. 02 Deposits Made Intact

Deposits are made intact?

Number of Answers: 1 Below 85% threshold: 1 Don't Know: 0 Not Applicable: 0

Vulnerability Category: Procedures

1. II. 01 Collections Deposited Daily

Collections are deposited daily?

Number of Answers: 1 Below 85% threshold: 1 Don't Know: 0 Not Applicable: 0

10. See Ideas For Collecting and Organizing Data, RiskWatch Phase IV - Reports on page 33 for discussion on Vulnerability Reports.

This concludes the Questions Phase.

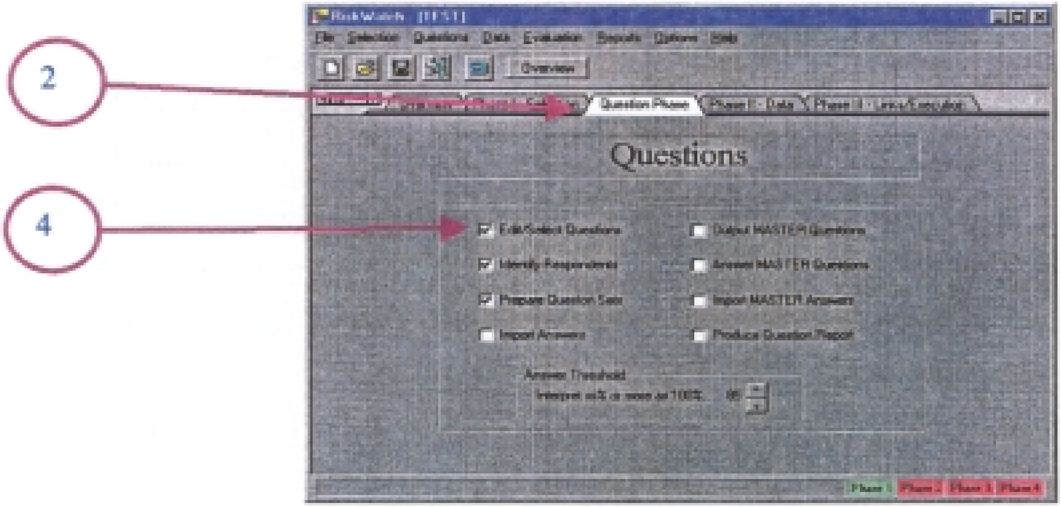
Question Phase How To Reference Guide

Import UINRAP Questions Category

Before building a question database, the analyst should import Unemployment Insurance National Risk Analysis Project (UINRAP) questions provided by the Department of Labor to all the SESAs.

Step by step instructions: Importing the UINRAP Questions:

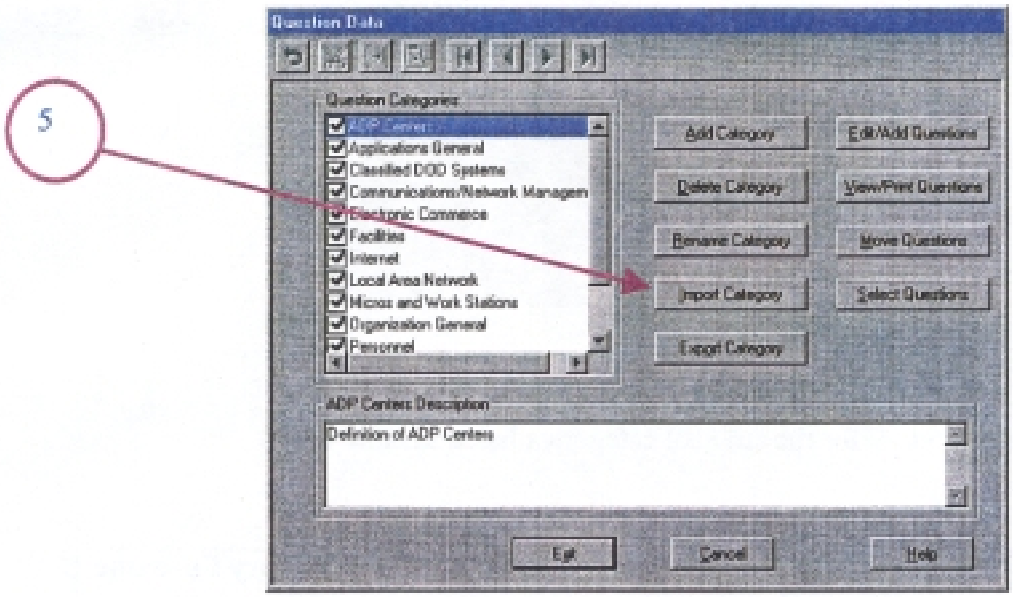
1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select **Question Phase** tab.
3. Place the UINRAP cassette in the A Drive.
4. Select **Edit / Select Questions**. The **Question Data** dialog box appears.



☑ Edit/Select Questions
☑ Identify Respondents
☑ Prepare Question Sets
☐ Import Answers
☐ Output MASTER Questions
☐ Answer MASTER Questions
☐ Import MASTER Answers
☐ Produce Question Report

Answer Threshold
Interpret xx% or more as 100% 95

5. Select **Import Category**. The **Import Category** dialog box appears.

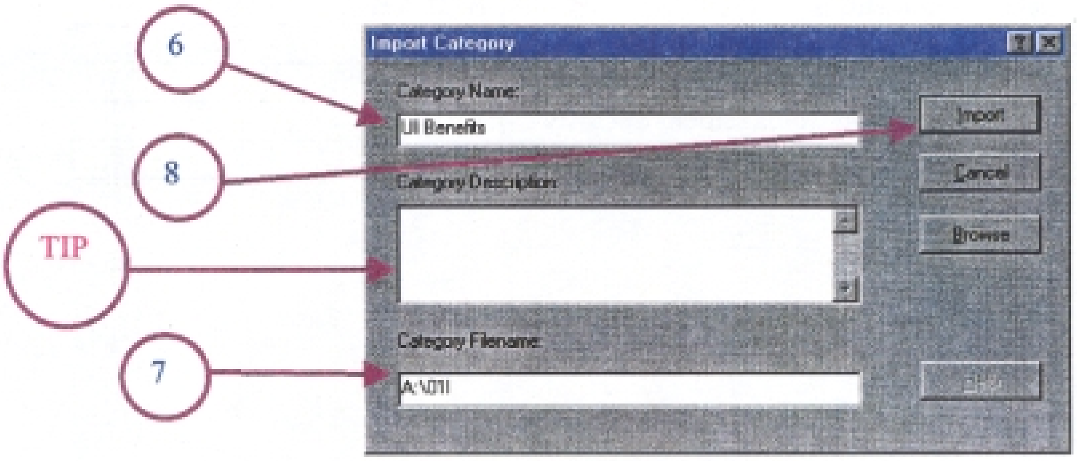


Question Categories:

- ☑ ADP Centers
- ☑ Applications General
- ☑ Classified DOD Systems
- ☑ Communications/Network Managem
- ☑ Electronic Commerce
- ☑ Facilities
- ☑ Internet
- ☑ Local Area Network
- ☑ Micros and Work Stations
- ☑ Organization General
- ☑ Personnel

ADP Centers Description: Definition of ADP Centers

6. Type "UI Benefits" in the **Category Name**.
7. Enter **A:\01I** (zero, one, capital I) in **Category Filename**.
8. Select **Import**.



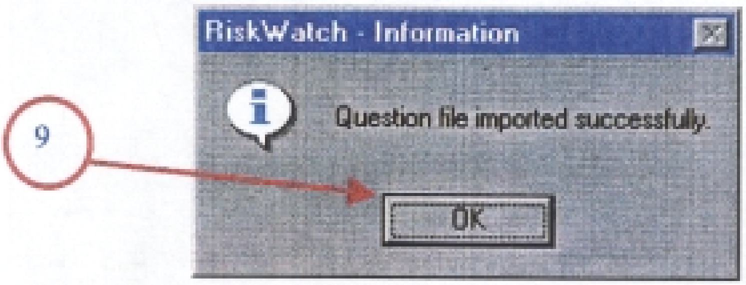
Category Name: UI Benefits

Category Description:

Category Filename: A:\01I

TIP
OPTIONAL: Enter a category description.

9. After importing the questions, RiskWatch displays the dialog box below. Select **OK.** RiskWatch returns to the **Import Category** dialog box.



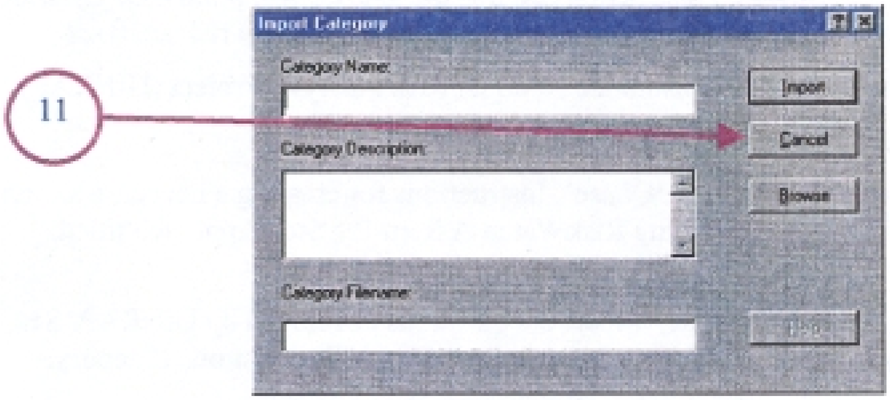
Question file imported successfully.

10. Repeat steps 6 to 9 for the ten (10) categories listed in table below.

Table 3 UINRAP Questions Category

Suggested Category Name **(Use in Step 6)**	**UINRAP Category Filename** **Use in Step 7**
UI Tax/Contributions	A:\02II
Field/Local Operations	A:\03III
Automated General Controls	A:\04IV
Application Controls	A:\05V
Automated System Controls	A:\06VI
Telecommunications	A:\07VII
Personal Computer (PC) Controls	A:\08VIII
Local and Wide Area Networks (LAN)	A:\09IV
Organizational and Management Security	A:\10X
Innovative Product Security	A:\11XI

11. After importing all categories, click **Cancel** to return to Question Data dialog box.



12. Select **Exit** to return to the Question Phase tab.

13. **File, Save.**

Building a Re-usable UI Question Database

By following the step-by-step instructions below, the analyst will build a UI question database, which is reusable and readily available for future agency risk analyses.

A. Importing Unemployment Insurance National Risk Analysis Project (UINRAP).

1. Start RiskWatch.
2. Create a new case named 'Qbase'. Instructions for creating a new case are on page 37 in the section Using RiskWatch A Step-By-Step Approach titled, Creating A Case.
3. While in the 'Qbase' case, import the questions developed by UINRAP. See page 106 for instructions on how to Import UINRAP Questions Category.

B. Create a Subdirectory in the RiskWatch directory called Qbase or any other appropriate name. Use this subdirectory to store the Question Database that is built.

4. Instructions for Using the Question Date Base for future use are included on page 111 of this manual.

C. Saving the Question Database.

5. Open the 'Qbase' case that was used to build the Questions database.
6. Minimize RiskWatch, but do not close RiskWatch.
7. If using Windows 95, open Windows Explorer. If using Windows 3.XX, open File Manager.
8. Locate the subdirectory in RiskWatch that was created in Step 4 above. The analyst will copy the files to this folder or subdirectory.
9. Open the "Qbase" directory in RiskWatch.
10. In the "Qbase" directory, locate the following files and highlight each:
    - qtables.db and qtables.px (Question DB)
    - ctables.db and ctables.px
11. Copy these files to the question database subdirectory created in Step 4 above. The analyst can also copy these files to diskette, if he/she choose.

Using the Question Date Base

Each time the analyst creates a case, the analyst can use the Question Database that was created above instead of starting from the beginning with modification to the RiskWatch questions. If the analyst choose to use the Question Database, simply copy the files to the new case.

1. Follow the steps for the Creating A Case on page 37.
2. Complete the steps required in Phase I - Selection and **Save** the case.
3. Minimize RiskWatch.
4. Locate the directory or folder where the Question Database was placed.
5. Highlight and copy the files to the folder or directory named after the new case.
6. **Save** and **Close** the case. When the analyst reopen the case, the question database will be present. Follow the Six Suggested Steps on page 79 to select the questions needed for this review.

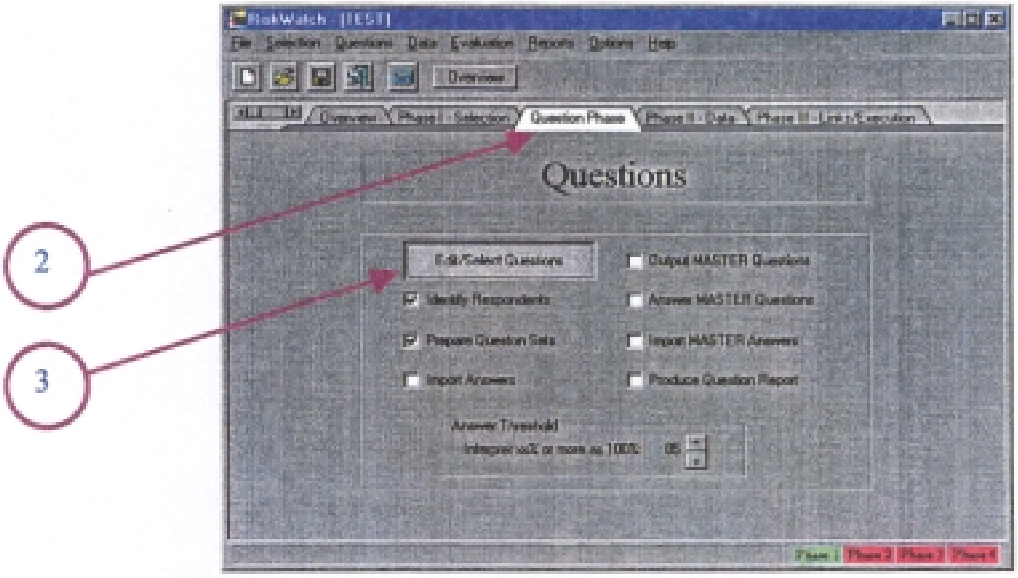
De-select Question Category

Deselecting a Question Category quickly removes the entire category of questions that do not apply to the analysis. Each time a new case is started, the analyst must deselect inappropriate categories because; RiskWatch selects all the question categories by default.

> EXAMPLE
> In the initial review of the business function under analysis, a supervisor informs the analyst that a LAN system is not used by the business function. Because the RiskWatch questionnaire program includes an entire question category on LAN systems, the analyst will want to remove that category from the analysis.

Step by step instructions: Deselecting Question Categories

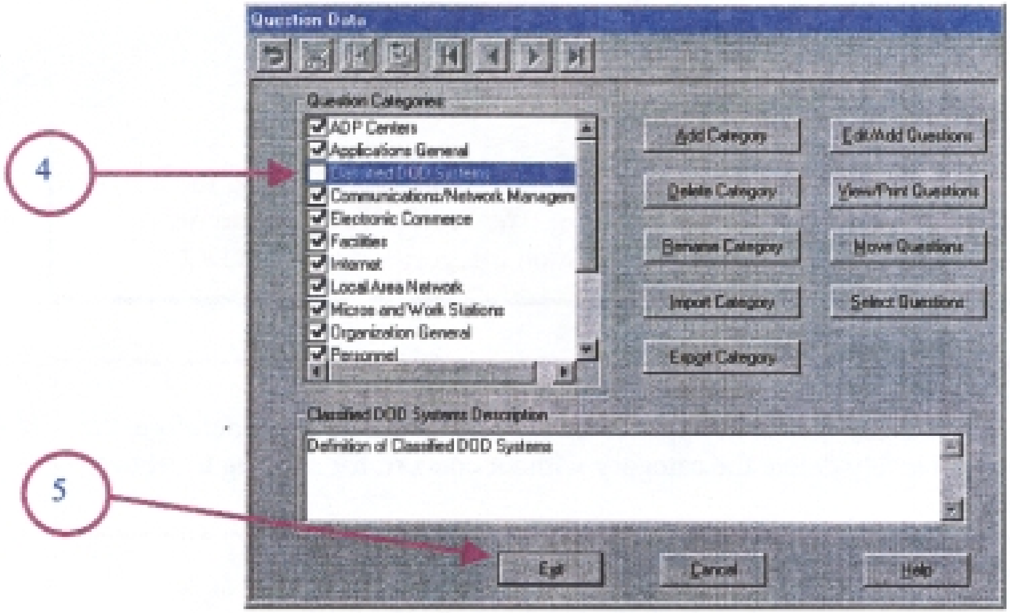
1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Click **Question Phase tab**.
3. Select **Edit/Select Questions**. The Question Data dialog box appears.



☑ Identify Respondents
☑ Prepare Question Sets
□ Import Answers
□ Output MASTER Questions
□ Answer MASTER Questions
□ Import MASTER Answers
□ Produce Question Report

Answer Threshold
Integer ≤ 0 or more as 100%: 85

4. Click the check mark next to the category(s) to **deselect** it.
5. Click **EXIT** after deselecting the question categories.



Question Categories:

- ☑ ADP Centers
- ☑ Applications General
- □ Classified DOD Systems
- ☑ Communications/Network Managem
- ☑ Electronic Commerce
- ☑ Facilities
- ☑ Internet
- ☑ Local Area Network
- ☑ Micros and Work Stations
- ☑ Organization General
- ☑ Personnel

Classified DOD Systems Description

Definition of Classified DOD Systems

TIP
When conducting risk analysis on UI systems, always deselect Classified DOD Systems. None of the DOD questions apply to Unemployment Insurance (UI) systems or functions.

Delete Question Category

OPTIONAL

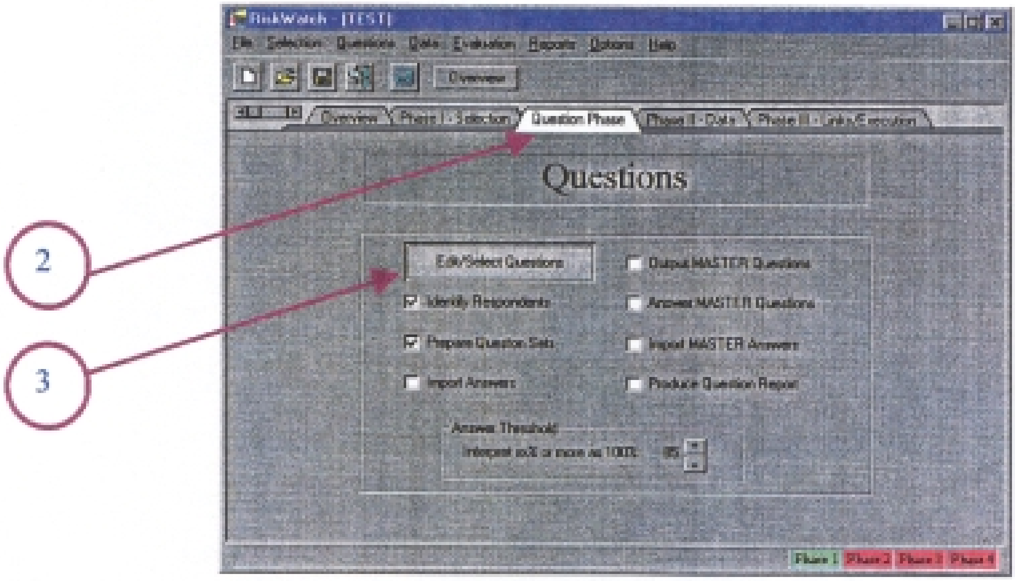
The purpose of deleting question categories is to completely remove the category from the listing of question categories.

> **WARNING**
> After the analyst deletes a Question Category, intentionally or not, the analyst cannot recover it for later use in the case. The Project Team recommends that beginning users not delete any question categories other than DOD.

> EXAMPLE
> None of the DOD questions apply to UI systems or functions. Therefore, the analyst can safely delete the category without concern for needing to recover it later.

Step by step instructions for deleting a Question Category

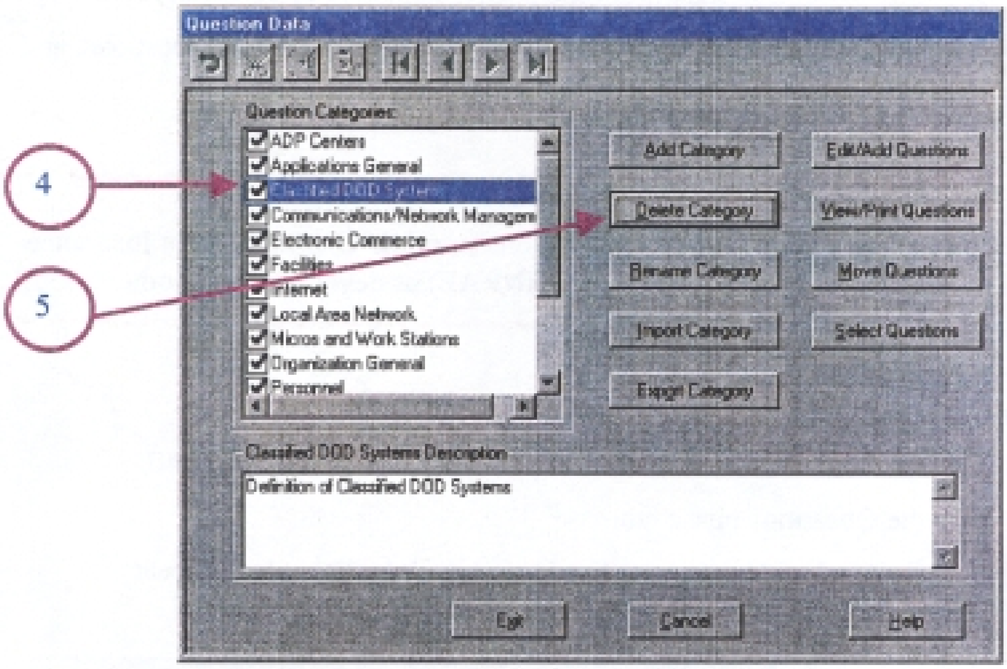
1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select **Question Phase tab.**
3. Select **Edit/Add questions**. The Question Data dialog box appears.



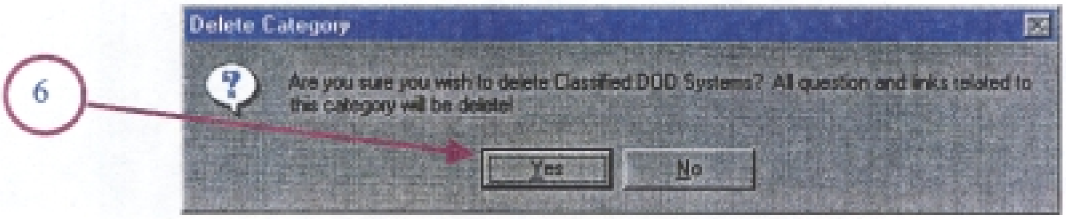
☑ Identify Respondents
☑ Prepare Question Sets
☐ Import Answers
☐ Output MASTER Questions
☐ Answer MASTER Questions
☐ Input MASTER Answers
☐ Produce Question Report

Answer Threshold
Interpret xx% or more as 100%: 85

4. **Click** on the name of the category to be deleted.
5. Click **Delete Category** button. A Delete Category dialog box appears.



6. If certain this category should be deleted, select **Yes** to confirm the deletion.



Are you sure you wish to delete Classified DOD Systems? All question and links related to this category will be delete!

Add Question Category

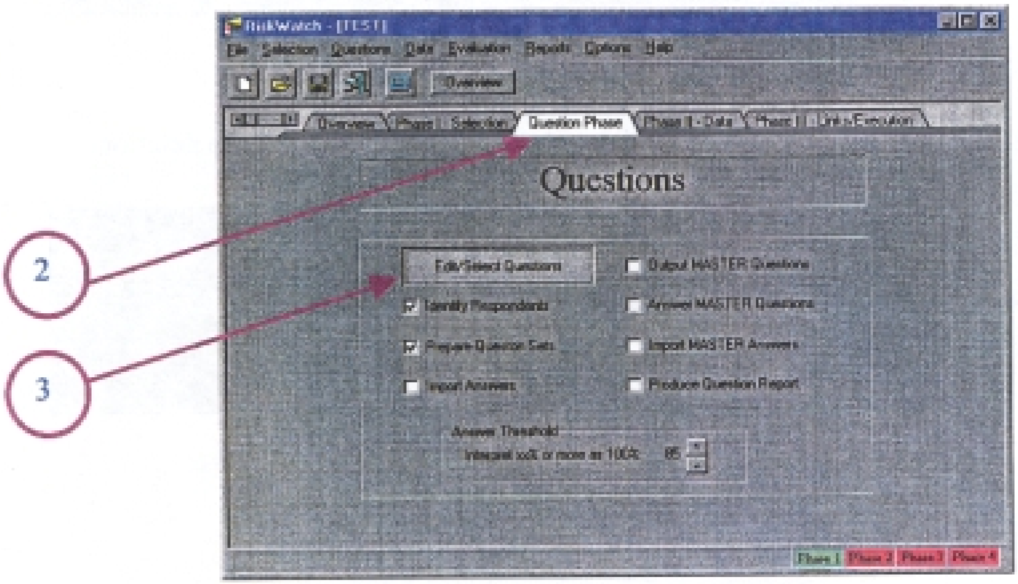
Adding a new question category provides:

- The ability to "tailor" the question category names to more closely fit the agency,
- A category in which to add new questions or to move existing questions, and
- A category in which to import questions.

> **Example**
> The analyst wants to import questions from the Unemployment Insurance National Risk Analysis Project (UINRAP) or developed by another SESA.

Step by step instructions: Adding a New Category Group Name:

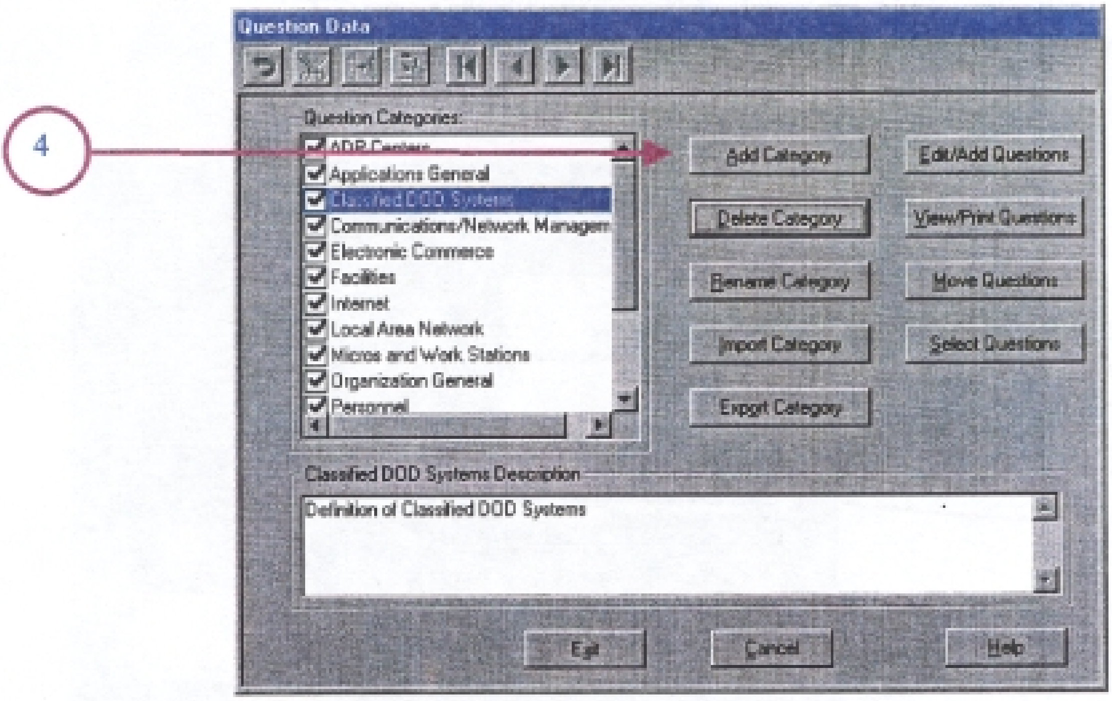
1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select the Questions phase tab.
3. Select **Edit/Select Questions**. The Question Data dialog box appears.



☑ Identify Respondents
☑ Prepare Question Sets
□ Import Answers
□ Output MASTER Questions
□ Answer MASTER Questions
□ Import MASTER Answers
□ Produce Question Report

Answer Threshold
Interpret xx% or more as 100%: 85

4. Select **Add Category**. The **Add Category** dialog box appears.

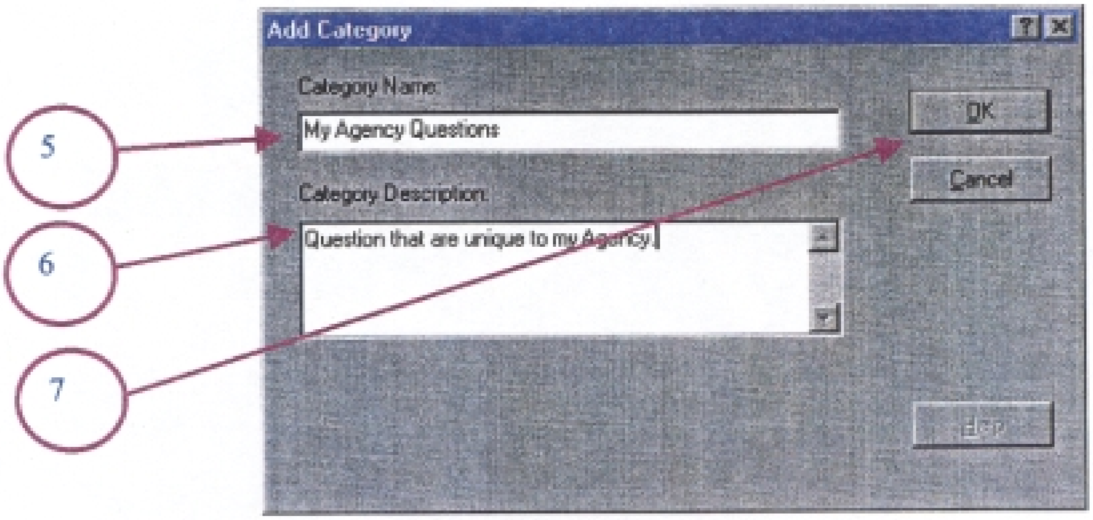


Classified DOD Systems Description: Definition of Classified DOD Systems

5. Type in the category name.

6. OPTIONAL: Type in a description of new category.

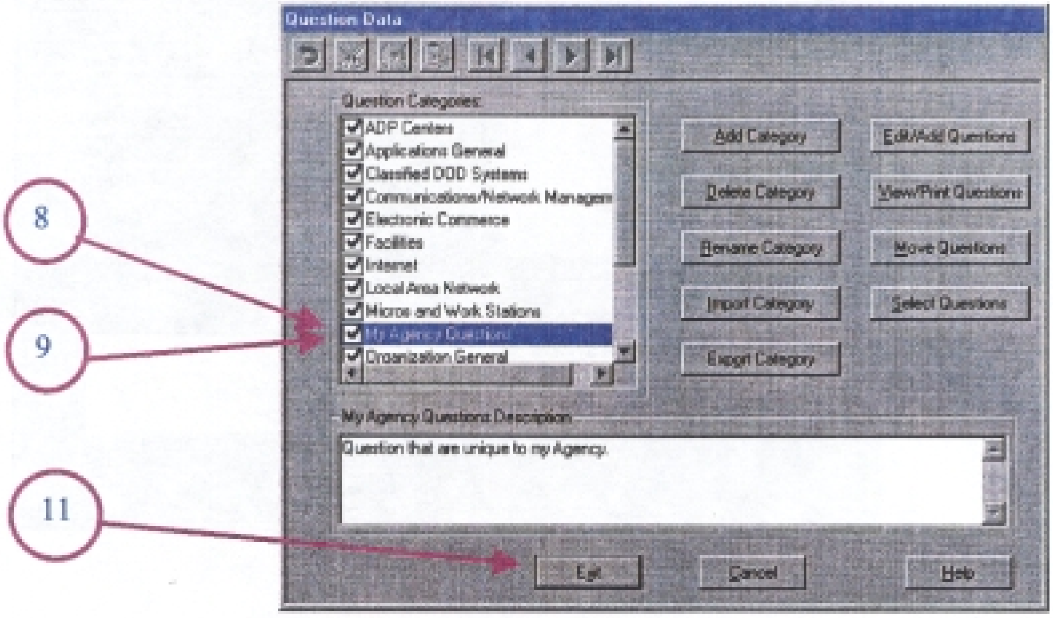
7. When finished, select **OK.** RiskWatch returns to the Question Data dialog box in which the new category appears.



Category Name: My Agency Questions

Category Description: Question that are unique to my Agency.

8. Click box next to the new category to select it.
9. Repeat steps 4 to 8 for each new Question Category.
10. When finished adding question categories, select **EXIT**.
11. **File, Save**



Question Categories:

- ☑ ADP Centers
- ☑ Applications General
- ☑ Classified DOD Systems
- ☑ Communications/Network Managem
- ☑ Electronic Commerce
- ☑ Facilities
- ☑ Internet
- ☑ Local Area Network
- ☑ Micros and Work Stations
- ☑ My Agency Questions
- ☑ Organization General

My Agency Questions Description

Question that are unique to my Agency.

Rename Question Category

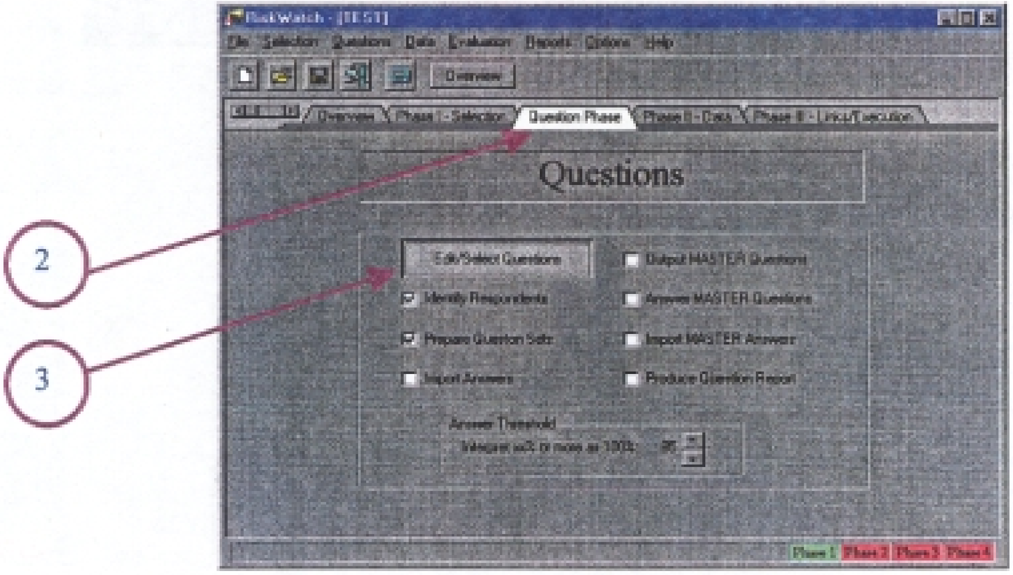
OPTIONAL

Renaming existing question categories changes category names to those that more closely match or fit the agency.

> EXAMPLE
> RiskWatch uses a category named ADP Centers, but your agency refers to this as the Operations Center. Therefore, the analyst changes the name to match that used in the agency (Operations Center).

Step by step instructions: Renaming Question Categories:

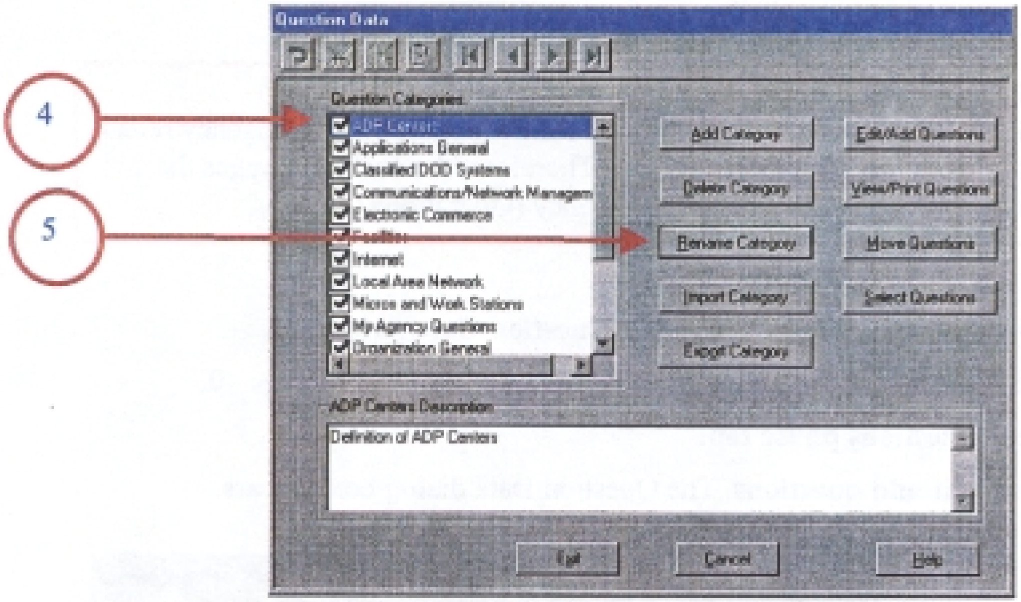
1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select **Questions phase tab**.
3. Select **edit/add questions.** The Question Data dialog box appears.



☐ Output MASTER Questions
☑ Identify Respondents
☐ Answer MASTER Questions
☑ Prepare Question Sets
☐ Import MASTER Answers
☐ Import Answers
☐ Produce Question Report

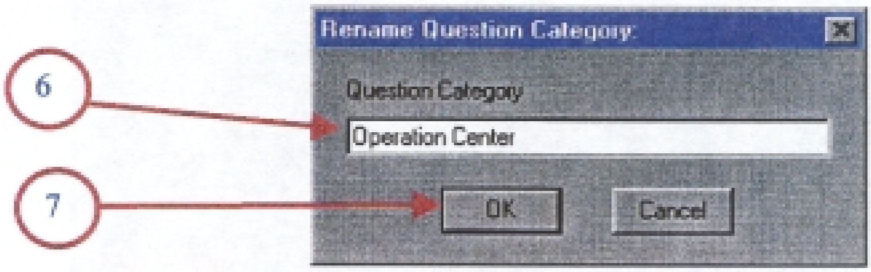
Answer Threshold
Integer >=0 or none as 100: 95

4. Highlight the **Question Category** to be renamed.
5. Click **Rename Category** button. The **Rename Question Category** dialog box appears.



ADP Centers Description: Definition of ADP Centers

6. Type in the new name for the category.
7. Click **O.K.** RiskWatch returns to the **Question Data** dialog box.



Question Category: Operation Center

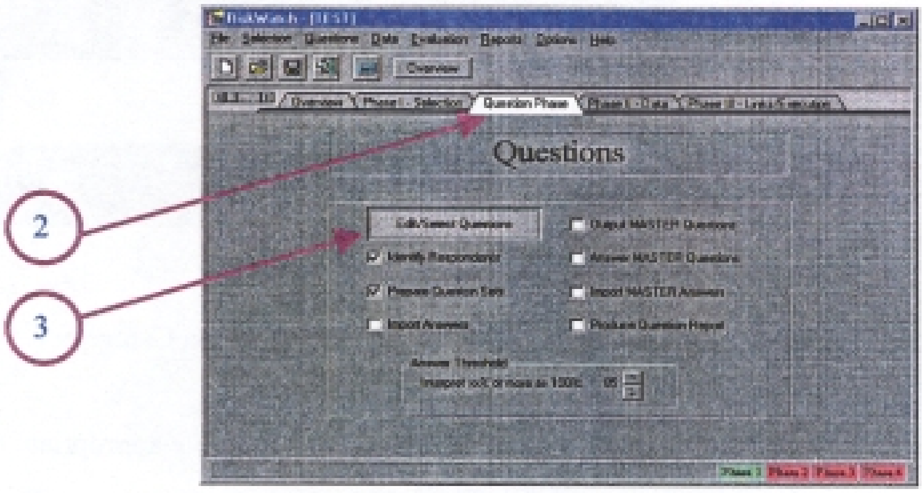
8. Repeat Steps 4 to 7 for each Question Category that needs to be renamed.
9. When finished, click on **Exit** to return to **Question Phase** tab.
10. **File, Save**.

Import Question Category

EXAMPLE
The analyst may have a diskette of UI questions developed by another SESA that can be used in the review case.

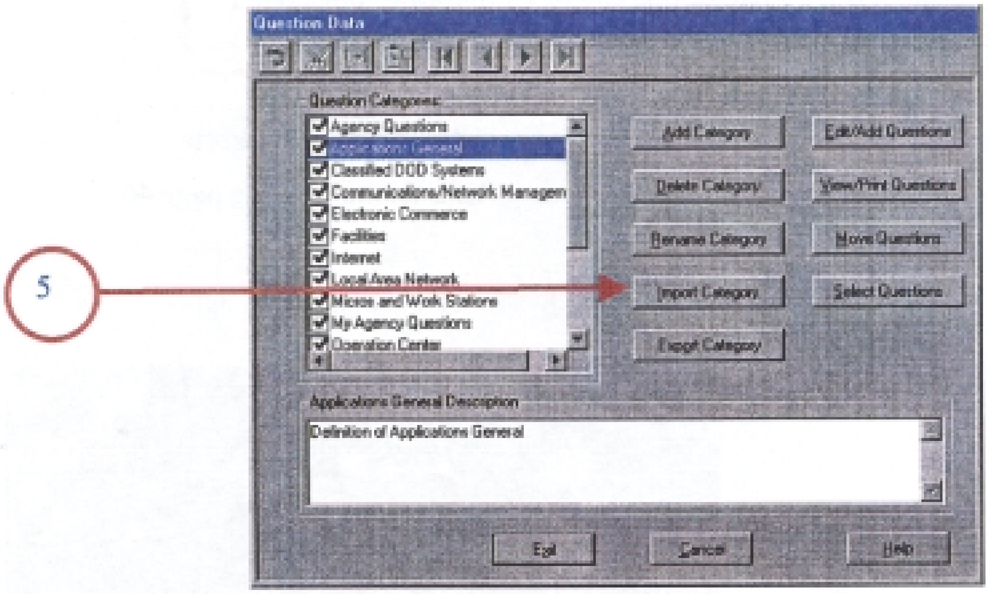
Step by step instructions: Importing questions from a diskette

1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select **Questions Phase** tab.
3. Select **edit/add questions**. The Question Data dialog box appears.



☑ Identify Respondents
☑ Prepare Question Sets
□ Import Answers
□ Output MASTER Questions
□ Answer MASTER Questions
□ Import MASTER Answers
□ Produce Question Report

4. Place the media with the questions for import into the corresponding drive.
5. Select **Import category**. The **Import Category** dialog box appears. In the Category Name box, type the Question Category name.

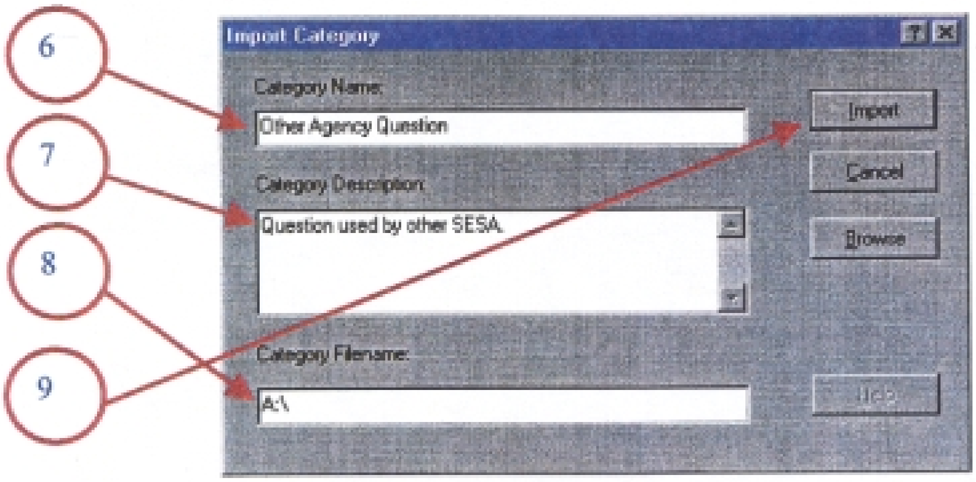


Question Categories:

- ☑ Agency Questions
- ☑ Applications General
- ☑ Classified DOD Systems
- ☑ Communications/Network Managem
- ☑ Electronic Commerce
- ☑ Facilities
- ☑ Internet
- ☑ Local Area Network
- ☑ Micros and Work Stations
- ☑ My Agency Questions
- ☑ Operation Center

Applications General Description: Definition of Applications General

6. In the **Category Name** box, type in the name of the Question Category.
7. OPTIONAL: Enter a **Category Description**.
8. In **Category Filename,** type the file name for import from the appropriate drive.
9. Select **Import**.



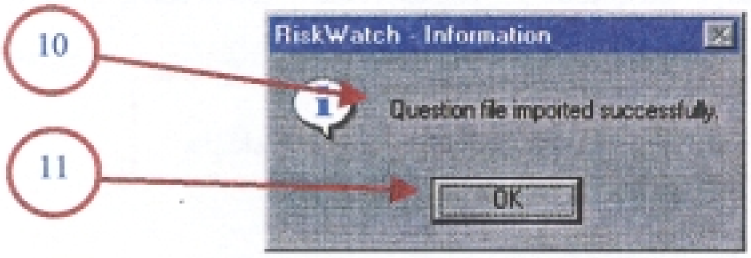
Category Name: Other Agency Question

Category Description: Question used by other SESA.

Category Filename: A:\

10. RiskWatch imports the questions and displays a dialog box stating "Question file imported successfully."

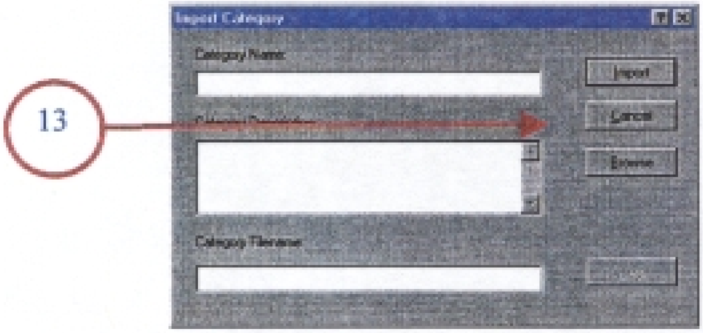
11. Select **OK.** The **Import Category** dialog box reappears.



Question file imported successfully.

12. Follow Steps 4 to 11 for each additional **Question Category** to import.

13. Click **Cancel** when finished to return to **Question Data** dialog box.



14. Click **Exit** to return to the **Question Phase** tab.

15. **File, Save.**

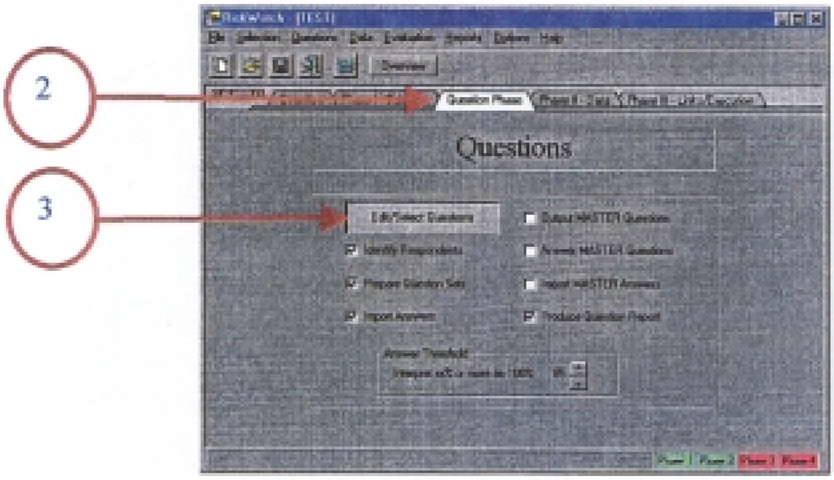
Export Question Category

Export Category allows the analyst to export categories one at a time to a specified drive/path. Categories are exported only from the "Master" RW directory. When using this menu item, the analyst has the option to indicate a different question category file name for the exported questions. The exported question category may then be imported using the Import Question function.

EXAMPLE
Place a Category onto a diskette, e: mail the file or mail the diskette.

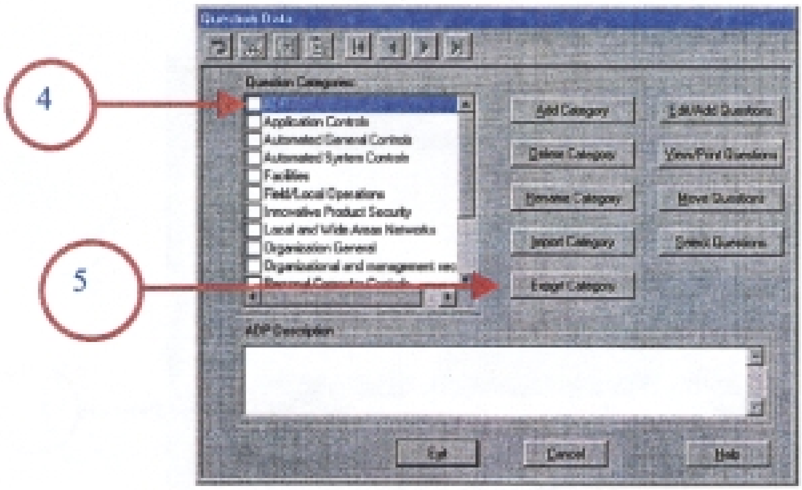
Step by step instructions: Export the Category

1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. **Select** the Question Phase tab.
3. **Click once** on top of Edit/Select Question. The Question Data dialog box appears.



☑ Identify Respondents
☑ Prepare Question Sets
☑ Import Answers
□ Output MASTER Questions
□ Answer MASTER Questions
□ Import MASTER Answers
☑ Produce Question Report

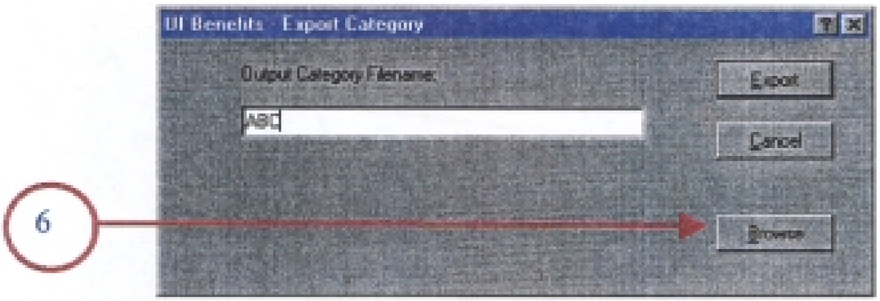
4. Highlight the Question Category to be exported.
5. Click **Export Category**, a dialog box appears with the Question Category name as part of the dialog box name.



Question Categories:
- □ ABC
- □ Application Controls
- □ Automated General Controls
- □ Automated System Controls
- □ Facilities
- □ Field/Local Operations
- □ Innovative Product Security
- □ Local and Wide Areas Networks
- □ Organization General
- □ Organizational and management sec
- □ Personal Computer Controls

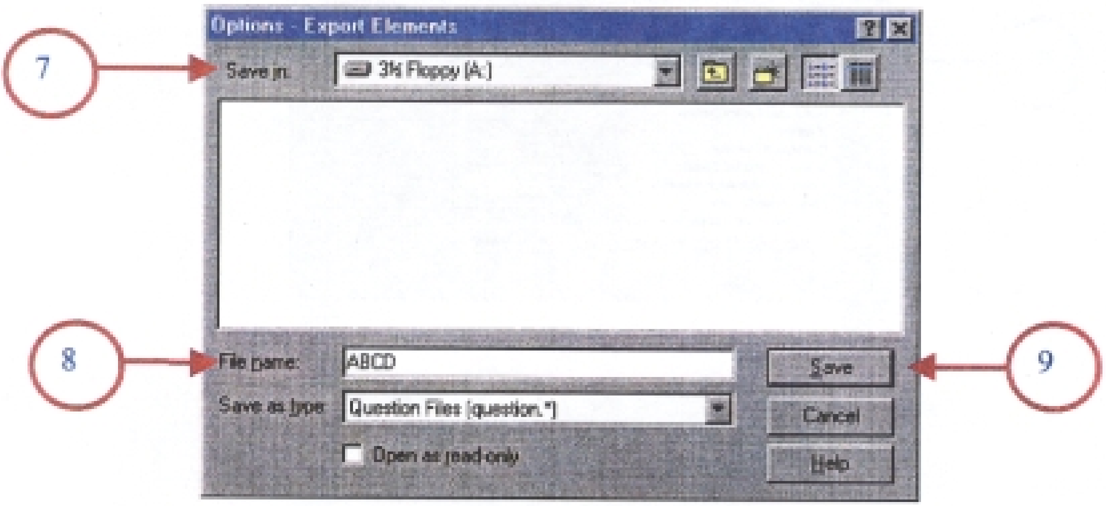
ADP Description

6. Click **Browse**. The **Options – Export Elements** dialog box appears.



Output Category Filename: ABC

7. In the **Save In** box, select the drive to which the file will be saved.
8. In the **File Name** box, enter the Question Category file name.
9. Click **Save.** The **Question – Export Category** reappears with the destination and file name entered.



Options - Export Elements

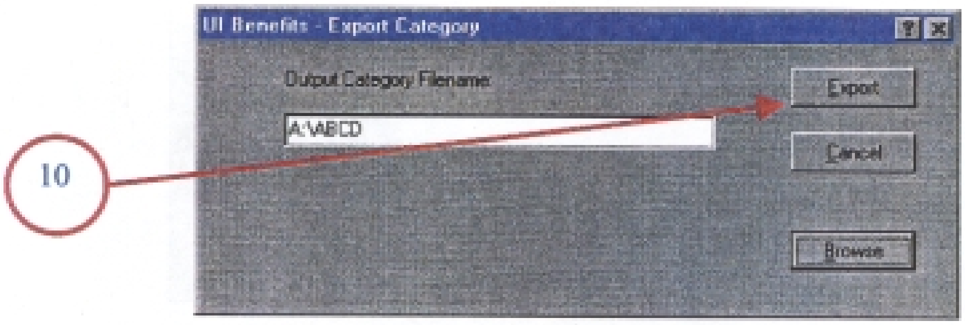
Save in: 3½ Floppy (A:)

File name: ABCD

Save as type: Question Files (question.*)

□ Open as read-only

10. Click **Export** to save file. The RiskWatch – Information dialog box appears.

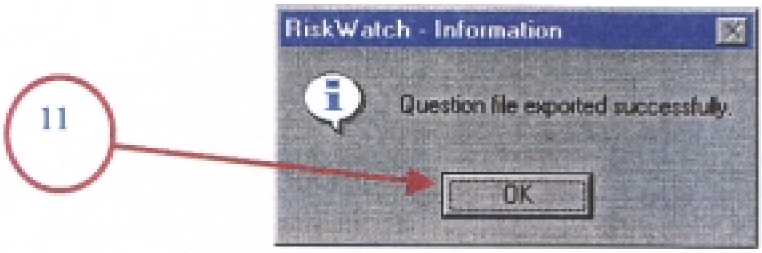


UI Benefits - Export Category

Output Category Filename

A:\ABCD

11. Click **O.K.** The Question Data dialog box reappears.



RiskWatch - Information

Question file exported successfully.

Adding Self-Developed Questions

Adding self-developed questions is intended for more experienced analysts.

Prior to any question development, the analyst should have an understanding of RiskWatch Question Sets. Question Sets always consists of three components:

1. A Control Standard

   A statement of a policy, a procedure, a security precaution, a commonly accepted business practice, etc., to which compliance is expected.

   EXAMPLE
   'Passwords must be changed every 90 days.'

2. A Question Statement

   Used to query respondents concerning the degree of compliance to a Control Standard. With RiskWatch, Question Statements are not phrased as questions, but phrased as a positive affirmation to the control standard.

   EXAMPLE
   'I change my password every 90 days.' This would be a suitable Question Statement to query respondents concerning the Control Standard: 'Passwords must be changed every 90 days.'

   TIP
   Respondents tend to answer 'Don't Know' to questions that are not phrased in the first person (I). When phrased with no subject or in the second (the analyst) or third person (he, she, they), the respondents tend to answer as though responding for the entire business function or agency.

3. A Vulnerability Statement

A Vulnerability Statement is phrased so that it shows a negative reflection of the Control Standard. When the RiskWatch program determines that, as a result of respondent's answers to the questionnaire program, a Control Standard is not being sufficiently complied with, the RiskWatch program will produce a report with a Vulnerability Statement.

EXAMPLE
'Passwords are not changed every 90 days.' This would be the vulnerability statement generated as a result of non-compliance answers to the Question Statement: 'Passwords are changed every 90 days.'

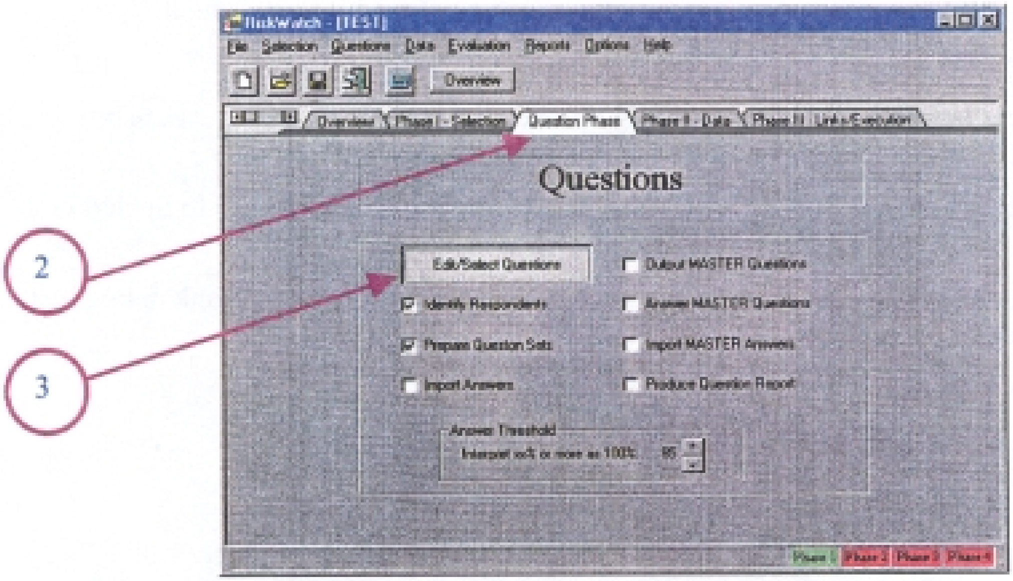
Question Sets are always developed by first stating a Control Standard, followed by a Question Statement, and ending with a Vulnerability Statement.

When adding new questions, information is supplied to following fields:

- Question Category - The analyst selects the Question Category most appropriate for the question.
- Question Title - The Question Title serves to identify and track the question. The words and numbers do not effect the program outcome.
- Vulnerability Area – The analyst selects the Vulnerability Area that best indicates the type of vulnerability addressed by the vulnerability statement. The analyst can select only one Vulnerability Area per question.
- Functional Areas – The analyst selects all the Functional Areas to which the question relates. The question can be linked to one or more Functional Areas. All respondents associated with the selected Functional Area(s) will receive the question.
- Question Weight -The Question Weight determines the importance or significance of the question. The higher the weight, the more important or significant the question. The default weight is one (1).

Step by step instructions: Self-developed Question Sets

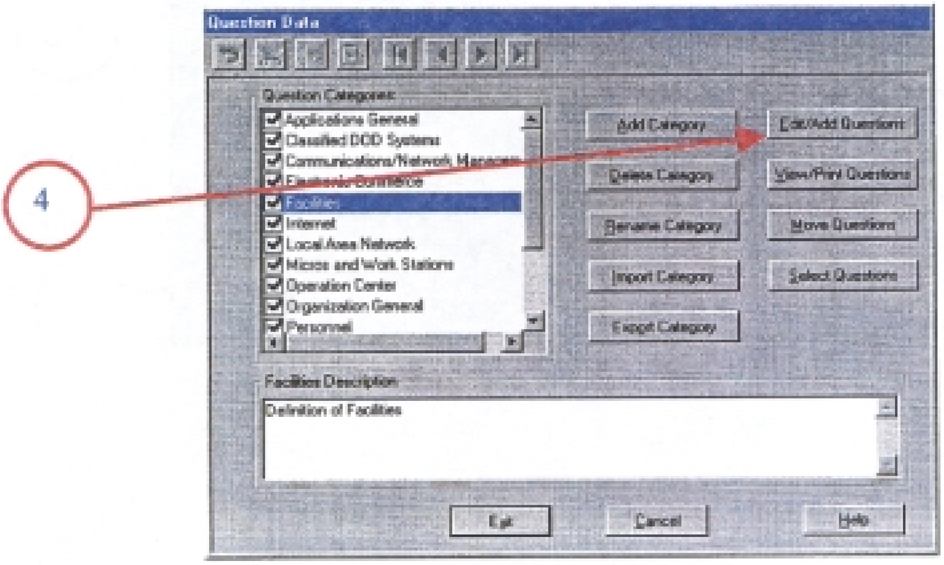
1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select **Question Phase tab**.
3. Select **Edit /Select**. The Question Data dialog box appears.



☑ Identify Respondents
☑ Prepare Question Sets
☐ Import Answers
☐ Output MASTER Questions
☐ Answer MASTER Questions
☐ Import MASTER Answers
☐ Produce Question Report

Interpret xx% or more as 100%: 85

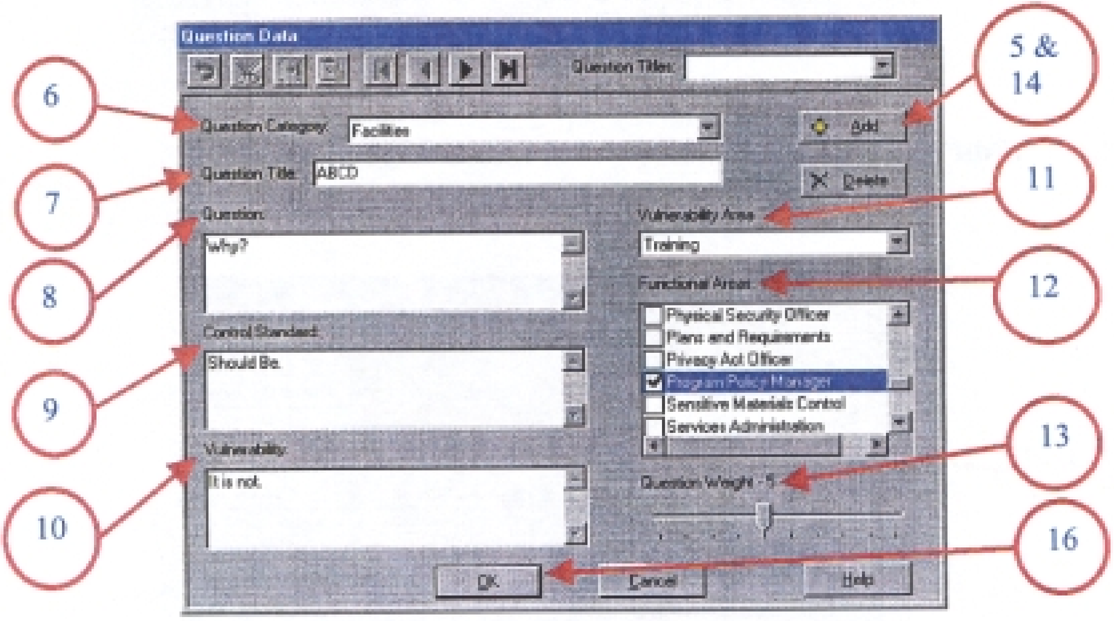
4. Click on **Edit/Add Questions**. The Question Data dialog box appears.



☑ Applications General
☑ Classified DOD Systems
☑ Communications/Network Managem
☑ Electronic Commerce
☑ Facilities
☑ Internet
☑ Local Area Network
☑ Micros and Work Stations
☑ Operation Center
☑ Organization General
☑ Personnel

Definition of Facilities

5. Click **Add**. A blank Question Data dialog box appears.
6. Using the pull down menu, select a **Question Category**.
7. In the **Question Title,** enter the question name.
8. In the **Question** box, enter the question.
9. In the **Control Standard** box, enter the question's control standard.
10. In the **Vulnerability** box, enter the question's vulnerability statement
11. Using the pull down menu, select a **Vulnerability Area**.
12. Select **Function Area** by scrolling up or down in the **Functional Areas** box and checking the box (es) to the left of the **Functional Area**.
13. Select **Question Weight** by sliding the downward pointing arrow to the left or right.
14. Click on **Add** when the new question has been entered. A new blank dialog box appears.
15. Repeat steps 6 to 14 until all new questions are entered.
16. Click **O.K.** RiskWatch returns to the Question Phase tab.



Question Data

Question Titles:

Question Category: Facilities

Question Title: ABCD

Question: why?

Control Standard: Should Be.

Vulnerability: It is not.

Vulnerability Area: Training

Functional Areas:
- □ Physical Security Officer
- □ Plans and Requirements
- □ Privacy Act Officer
- ☑ Program Policy Manager
- □ Sensitive Materials Control
- □ Services Administration

Question Weight - 5

17. **File, Save**

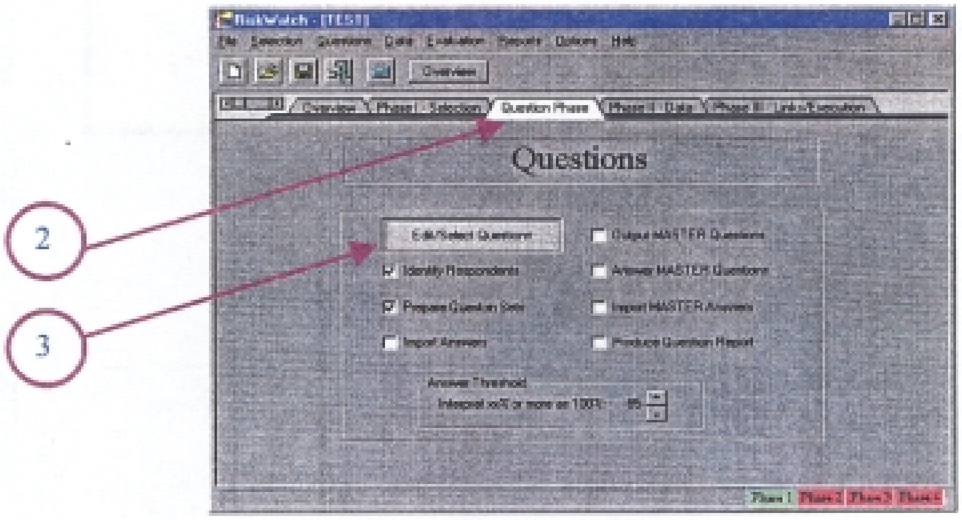
Modify Individual Questions

From the printed copy of the modified questions, the analyst edits the RiskWatch question database.

WARNING
Beginning RiskWatch users should modify as few words as possible in the Question, Control Statement, and Vulnerability boxes. If major changes are necessary, consider developing a new question following the instructions for Adding Self-Developed Questions.

Step by step instructions: Modifying Questions in RiskWatch:

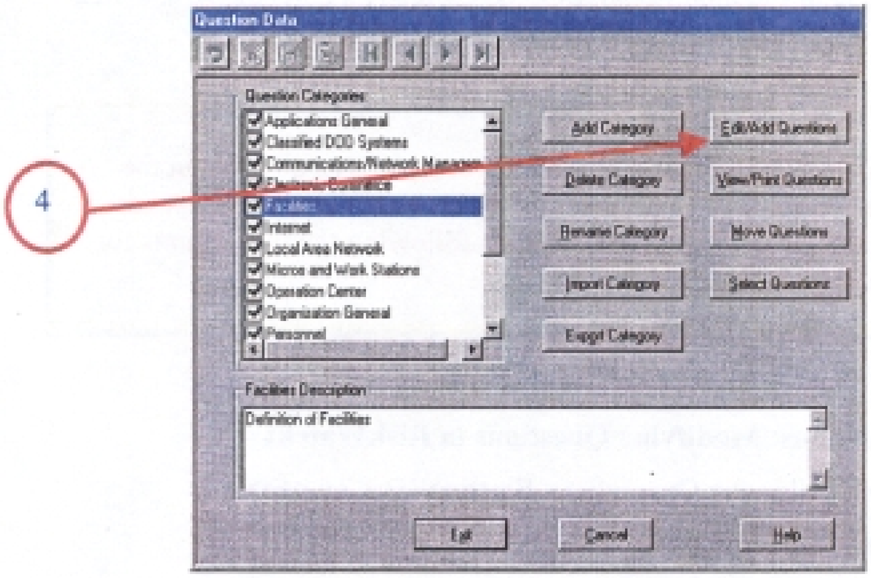
1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select **Question Phase tab.**
3. Select **Edit/Select Questions**, The Question Data dialog box appears.



☑ Identify Respondents
☑ Prepare Question Sets
☐ Import Answers
☐ Output MASTER Questions
☐ Answer MASTER Questions
☐ Import MASTER Answers
☐ Produce Question Report

Interpret xx% or more as 100%: 85

4. Select **Edit/Add Questions**, a different Question Data box appears.



Question Categories:

☑ Applications General
☑ Classified DOD Systems
☑ Communications/Network Managem
☑ Electronic Commerce
☑ Facilities
☑ Internet
☑ Local Area Network
☑ Micros and Work Stations
☑ Operation Center
☑ Organization General
☑ Personnel

Facilities Description

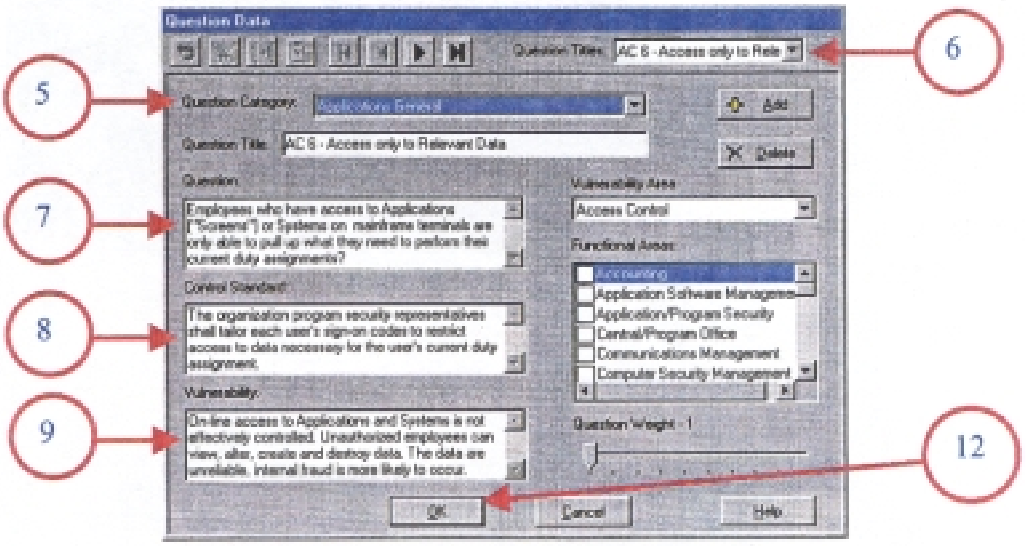
Definition of Facilities

WARNING
Save often. In version 7.1, return to the Question Phase tab to save. Do a **Save** after editing each question category.

5. Select the **Question Category** to be modified from the "Question Category" box by clicking on the pull down menu.
6. Select the question to be modified from the **Question Titles** box using pull down menu.
7. Highlight and delete the text to be changed in the **Question** box. Then type in the new text to fit the organization or business function.
8. Highlight and delete the text to be changed in the **Control Standard** box. Then type in the new text to fit the organization or business function.
9. Highlight and delete the text to be changed in the **Vulnerability Statement** box. Then type in the new text to fit the organization or business function.

WARNING
When editing questions in RiskWatch, the analyst must remember to edit not only the question but also the control standard and the vulnerability statement. If this is not done, the Vulnerability Reports will not be correctly phrased.

10. Repeat steps 6 to 9 as often as necessary for the selected **Question Category**.
11. Return to step 5 to select the next Question Category and continue modifying the questions.
12. Repeat Steps 3 to 11 until all necessary edits are completed. Select **OK** to return to the Question Phase tab.
13. **File, Save.**



Question Titles: AC 6 - Access only to Rele

Question Category: Applications General

Question Title: AC 6 - Access only to Relevant Data

Question:
Employees who have access to Applications ("Screens") or Systems on mainframe terminals are only able to pull up what they need to perform their current duty assignments?

Control Standard:
The organization program security representatives shall tailor each user's sign-on codes to restrict access to data necessary for the user's current duty assignment.

Vulnerability:
On-line access to Applications and Systems is not effectively controlled. Unauthorized employees can view, alter, create and destroy data. The data are unreliable, internal fraud is more likely to occur.

Vulnerability Area: Access Control

Functional Areas:
□ Accounting
□ Application Software Manageme
□ Application/Program Security
□ Central/Program Office
□ Communications Management
□ Computer Security Management

Question Weight - 1

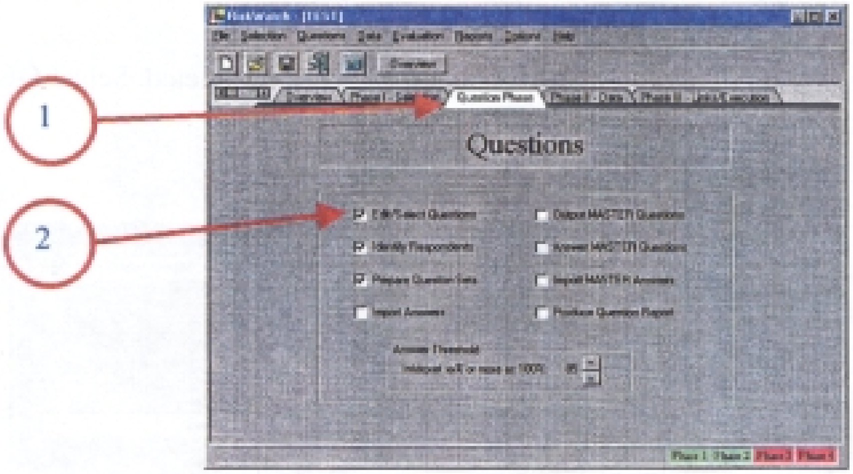
Select Individual Question

The **Select Individual Question** process requires the analyst to use a two step process. Using the annotated copy of the questions, the first step is deselecting the question that was determined not applicable to the agency or business function. In the second step, the analyst edits the **Vulnerability Area**, **Functional Areas**, and **Question Weight**.

> WARNING
> A question cannot be modified from the Select Questions screen. The user must use the Modify Individual Questions option to make modifications, as described on page 131.

Step 1. Step by step instructions: Selecting Individual Questions.

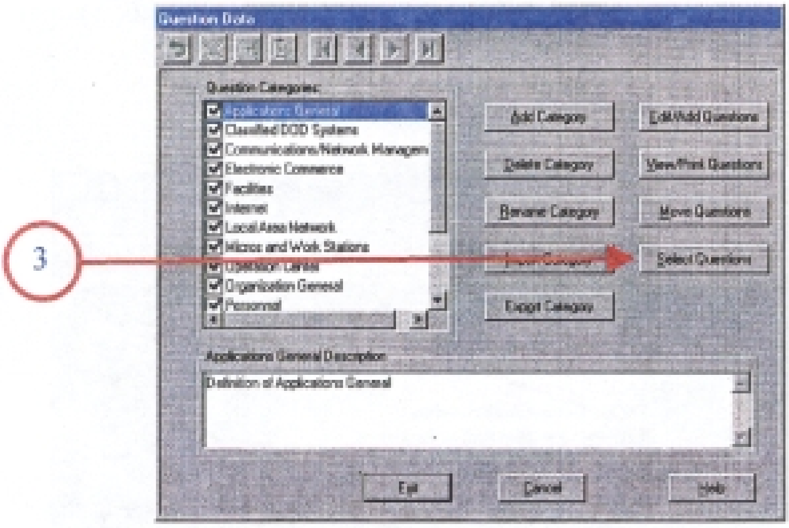
1. **Open** RiskWatch following Opening An Existing Case on page 40. Select the **Question Phase** tab.
2. Select **Edit/Select Questions**. The Question Data dialog box appears.


1
2
RiskWatch - [TEST]
File Selection Questions Data Evaluation Reports Options Help
Overview
Overview
Phase I - Selection
Question Phase
Phase II - Data
Phase III - Job Execution
Questions
Phase 1 Phase 2 Phase 3 Phase 4

☑ Edit/Select Questions
☑ Identify Respondents
☑ Prepare Question Sets
☐ Import Answers
☐ Output MASTER Questions
☐ Answer MASTER Questions
☐ Import MASTER Answers
☐ Produce Question Report

Answer Threshold
Interpret as 0 or more as 100% 85

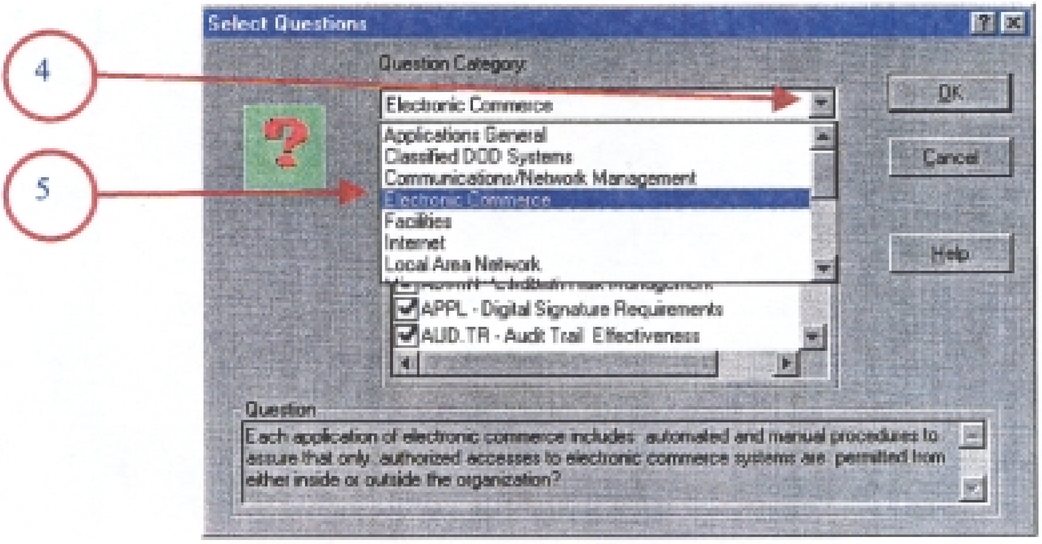
3. Click **Select Questions**. The Select Question dialog box appears.



Definition of Applications General

4. Use the pull down menu to select a **Question Category**.

5. Click once on the **Question Category** to highlight. RiskWatch lists the question titles for the selected category.



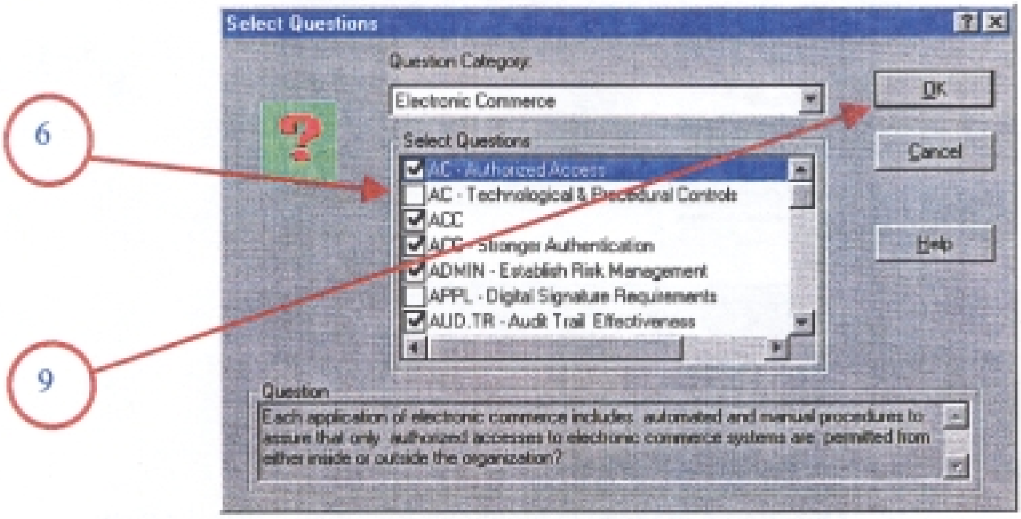
☑ APPL - Digital Signature Requirements

☑ AUD.TR - Audit Trail Effectiveness

Question

Each application of electronic commerce includes: automated and manual procedures to assure that only authorized accesses to electronic commerce systems are permitted from either inside or outside the organization?

6. Click the box next to the question that needs to be deselected.
7. Repeat Step 6 until all inappropriate questions in the category deselected.
8. Repeat steps 4 to 7 for each Question Category, if appropriate, then continue to Step 9 for the second step in Selecting Individual Questions.
9. Click **O.K.** to return to the Question Data dialog box.



Question Category: Electronic Commerce

Select Questions

- ☑ AC - Authorized Access
- □ AC - Technological & Procedural Controls
- ☑ ACC
- ☑ ACC - Stronger Authentication
- ☑ ADMIN - Establish Risk Management
- □ APPL - Digital Signature Requirements
- ☑ AUD.TR - Audit Trail Effectiveness

Question

Each application of electronic commerce includes: automated and manual procedures to assure that only authorized accesses to electronic commerce systems are permitted from either inside or outside the organization?

10. Click **Exit** to return to Question Phase tab.
11. **File, Save**

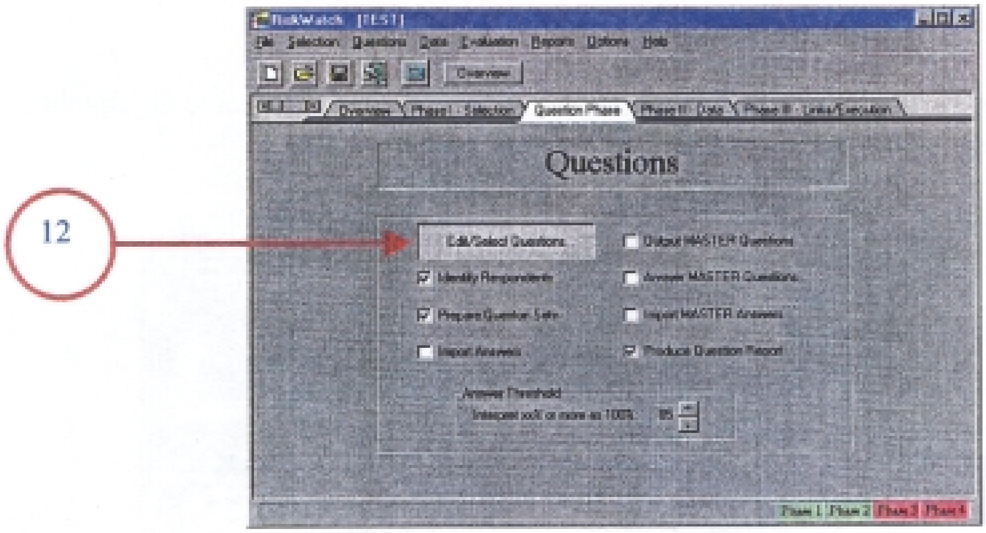
Vulnerability Area, Functional Area and Weight

The next procedure in the Select Individual Question involves sequential steps in choosing the **Vulnerability Area, Functional Area** and **Question Weight**.

> WARNING
> In the previous process, questions inappropriate to your agency or business function were deselected. In the next process, these deselected questions will still appear in the pull down menu; however, do not deselect the questions again.

Step 2. Step by step instructions: Selecting Individual Questions.

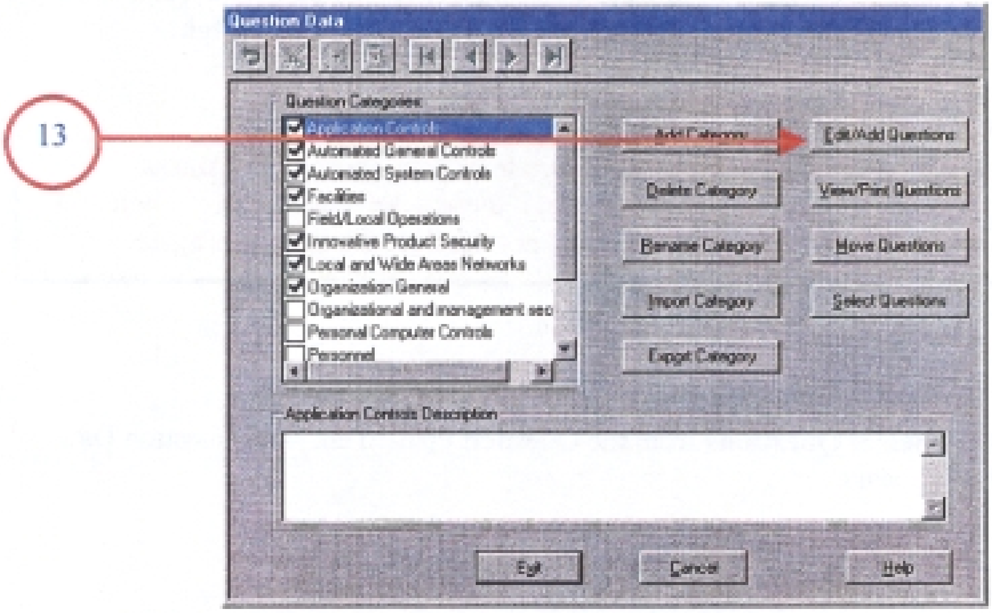
12. Select **Edit/Select Questions** from the Question Phase Tab. The Question Data dialog box appears.



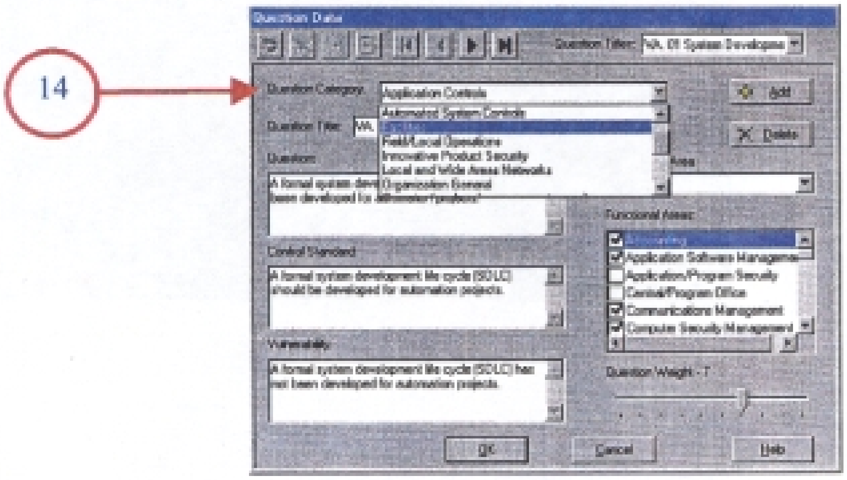
☑ Identify Respondents
☑ Prepare Question Sets
☐ Import Answers
☐ Output MASTER Questions
☐ Answer MASTER Questions
☐ Import MASTER Answers
☑ Produce Question Report

Answer Threshold
Interpret xx% or more as 100% 85

13. Select the **Edit/Add Questions** button. A different Question Data dialog box appears.



14. Select the **Question Category** by clicking the pull-down menu and highlighting the category.

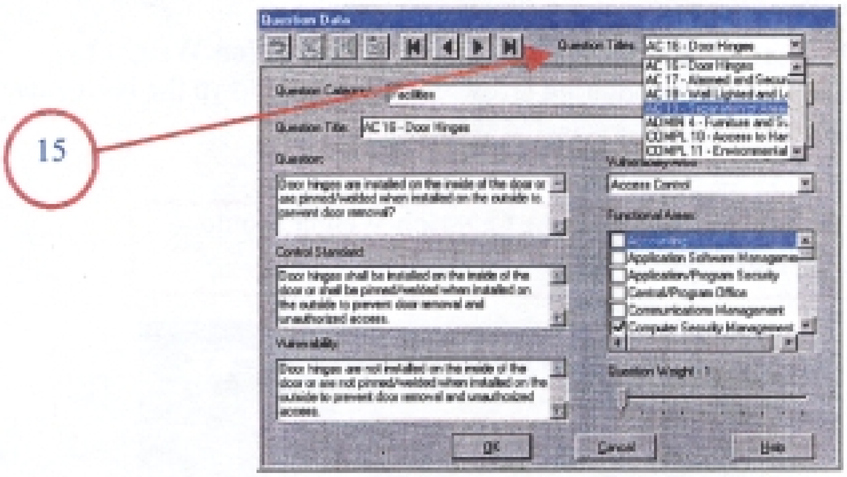

14
Question Data
Question Title: NA. 01 System Developme
Question Category: Application Controls
Automated System Controls
Facilities
Field/Local Operations
Innovative Product Security
Local and Wide Areas Networks
Organization General
Add
Delete
Question Title: NA.
Question:
Area
Functional Areas:
☑ Accounting
☑ Application Software Manageme
□ Application/Program Security
□ Central/Program Office
☑ Communications Management
☑ Computer Security Management
Question Weight - 7
OK
Cancel
Help

Question: A formal system deve… been developed for automation projects?

Control Standard: A formal system development life cycle (SDLC) should be developed for automation projects.

Vulnerability: A formal system development life cycle (SDLC) has not been developed for automation projects.

15. Select the **Question Title** by clicking the pull-down menu and highlighting the question.



Question Titles: AC 16 - Door Hinges
AC 16 - Door Hinges
AC 17 - Alarmed and Secur
AC 18 - Well Lighted and L
AC 19 - [illegible]
ADMIN 4 - Furniture and S
COMPL 10 - Access to Har
COMPL 11 - Environmental

Question Category: Facilities

Question Title: AC 16 - Door Hinges

Question: Door hinges are installed on the inside of the door or are pinned/welded when installed on the outside to prevent door removal?

Control Standard: Door hinges shall be installed on the inside of the door or shall be pinned/welded when installed on the outside to prevent door removal and unauthorized access.

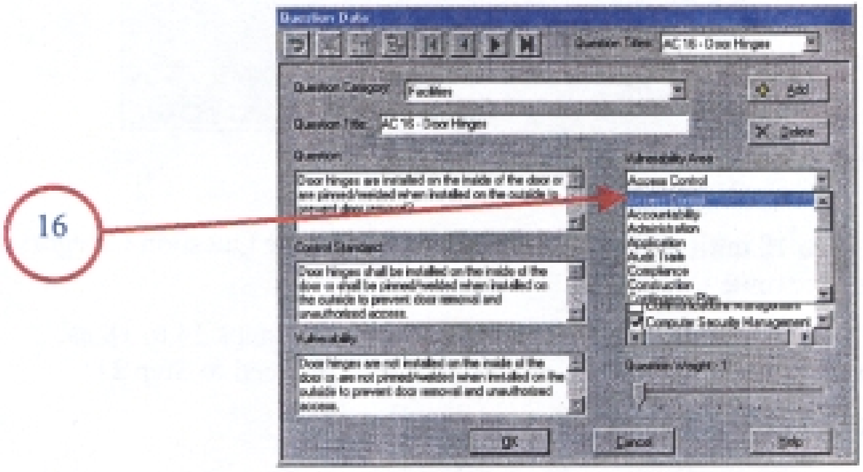
Vulnerability: Door hinges are not installed on the inside of the door or are not pinned/welded when installed on the outside to prevent door removal and unauthorized access.

Vulnerability Area: Access Control

Functional Areas:
□ Accounting
□ Application Software Management
□ Application/Program Security
□ Central/Program Office
□ Communications Management
☑ Computer Security Management

Question Weight : 1

16. If the default **Vulnerability Area** needs to be changed, select the **Vulnerability Area** by clicking the pull-down menu and highlighting the new vulnerability area.



Question Titles: AC 16 - Door Hinges

Question Category: Facilities

Question Title: AC 16 - Door Hinges

Question: Door hinges are installed on the inside of the door or are pinned/welded when installed on the outside to prevent door removal?

Control Standard: Door hinges shall be installed on the inside of the door or shall be pinned/welded when installed on the outside to prevent door removal and unauthorized access.

Vulnerability: Door hinges are not installed on the inside of the door or are not pinned/welded when installed on the outside to prevent door removal and unauthorized access.

Vulnerability Area: Access Control
Access Control
Accountability
Administration
Application
Audit Trails
Compliance
Construction
Contingency Plan

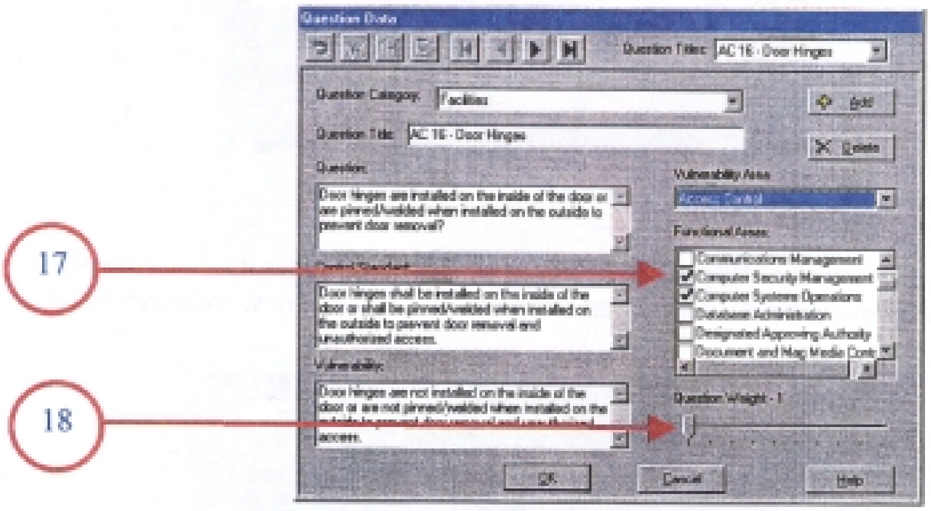
☑ Computer Security Management

Question Weight : 1

17. If the **Functional Areas** need to be changed, select the **Functional Area(s)** by placing the cursor on the box next to the Functional Area that is associated with the question. A check in the box means the Functional Area is selected; no check means it is deselected.

18. If the **Question Weight** needs to be changed, select the **Question Weight** by placing the cursor on the down-pointing arrow while holding down the left mouse button and sliding the arrow to the selected weight.

A RiskWatch Trainer indicated that the Question Weight should remain at 1 if the analyst lacks experience in risk analysis.



Question Titles: AC 16 - Door Hinges

Question Category: Facilities

Question Title: AC 16 - Door Hinges

Question:
Door hinges are installed on the inside of the door or are pinned/welded when installed on the outside to prevent door removal?

Control Standard:
Door hinges shall be installed on the inside of the door or shall be pinned/welded when installed on the outside to prevent door removal and unauthorized access.

Vulnerability:
Door hinges are not installed on the inside of the door or are not pinned/welded when installed on the outside to prevent door removal and unauthorized access.

Vulnerability Area: Access Control

Functional Areas:
- □ Communications Management
- ☑ Computer Security Management
- ☑ Computer Systems Operations
- □ Database Administration
- □ Designated Approving Authority
- □ Document and Mag Media Cont

Question Weight - 1

19. Repeat Steps 14 to 18 until all the necessary changes for the Question Category are complete. Then continue to step 20.

20. Repeat Step 13 for the next Question Category and follow steps 14 to 18 as needed. After completing all the Question Categories proceed to Step 21.

21. Click **O.K.** to return to Question Data dialog box.

22. Click **Exit** to return to the Question Phase tab.

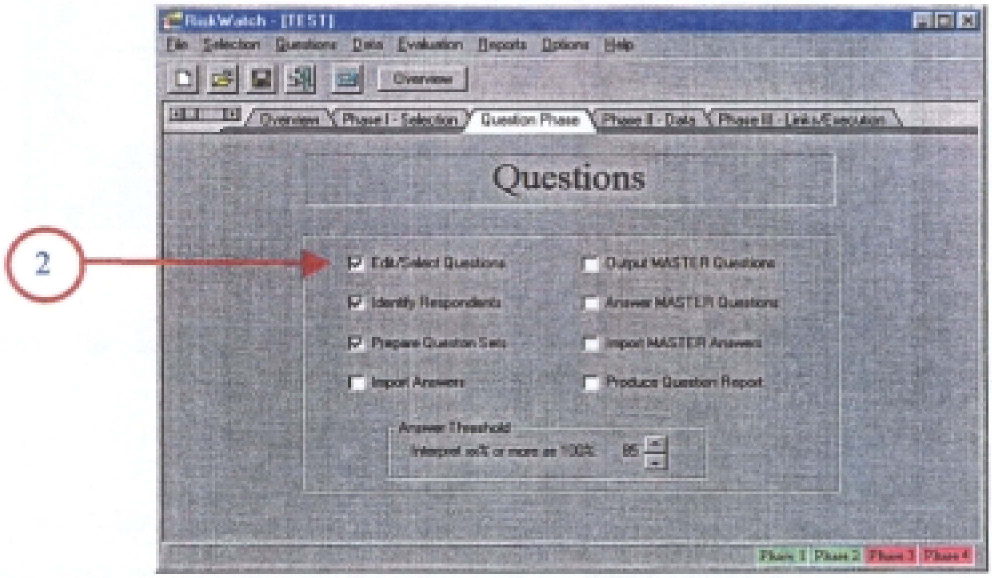
23. **File, Save.**

Moving Individual Question

Moving a question allows the user to place a question from one category to another, more appropriate, category. In some instances, it is easier for the analyst to move one or two questions to a more appropriate question category than to keep an entire unusable question category.

Step by step instructions: To moving a question:

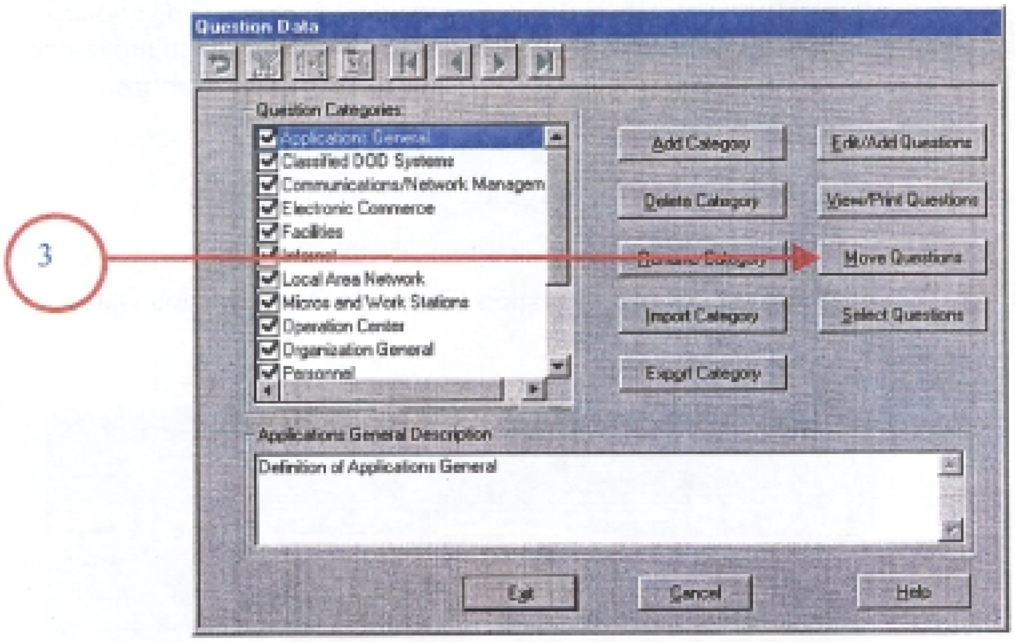
1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. Select **Edit/Select Question** from the Question Phase tab. The Question Data dialog box appears.



☑ Edit/Select Questions
☑ Identify Respondents
☑ Prepare Question Sets
□ Import Answers
□ Output MASTER Questions
□ Answer MASTER Questions
□ Import MASTER Answers
□ Produce Question Report

Answer Threshold
Interpret xx% or more as 100%: 85

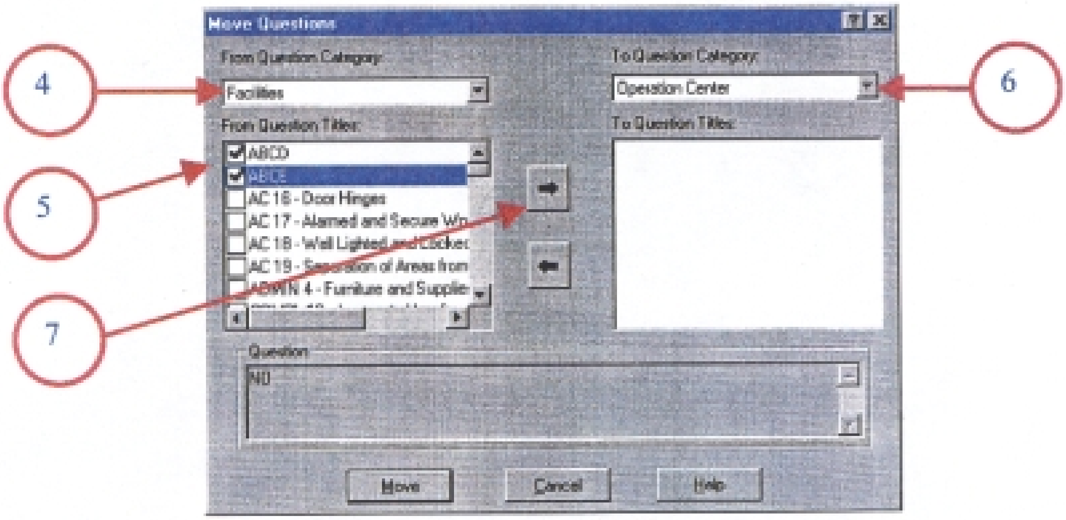
3. Click **Move Question** button. The Move Question dialog box appears.



Question Categories:
☑ Applications General
☑ Classified DOD Systems
☑ Communications/Network Managem
☑ Electronic Commerce
☑ Facilities
☑ Internet
☑ Local Area Network
☑ Micros and Work Stations
☑ Operation Center
☑ Organization General
☑ Personnel

Applications General Description
Definition of Applications General

4. Select a category from the **From Question Category** by using the pull-down menu.
5. In the **From Question Titles** box, place a check mark in box next to the question(s) needing to be moved.
6. Select the new category from **To Question Category** using the pull-down menu.
7. Click the **right-pointing arrow** once to move the question into the **To Question Titles** box.



From Question Category: Facilities

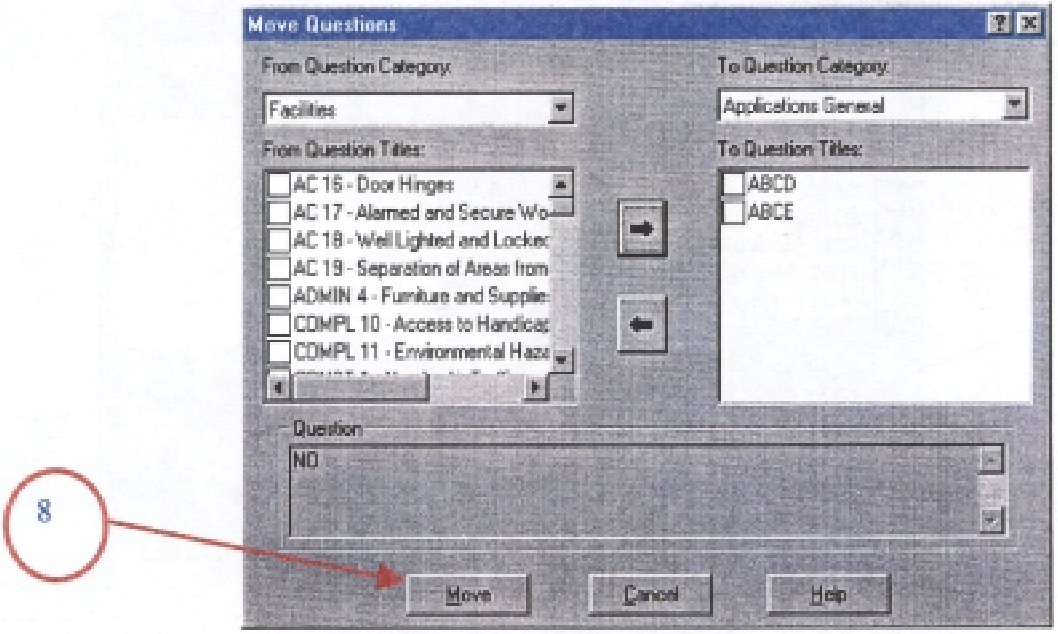
From Question Titles:
☑ ABCD
☑ ABCE
□ AC 16 - Door Hinges
□ AC 17 - Alarmed and Secure Wo
□ AC 18 - Well Lighted and Locked
□ AC 19 - Separation of Areas from
□ ADMIN 4 - Furniture and Supplie

To Question Category: Operation Center

To Question Titles:

Question
NO

8. Click the **Move** button after verifying the correct questions were moved to the **To Question Titles** box. A **Move Questions** dialog box appears asking if the analyst is sure he/she wishes to move the questions.



Move Questions

From Question Category: Facilities

To Question Category: Applications General

From Question Titles:

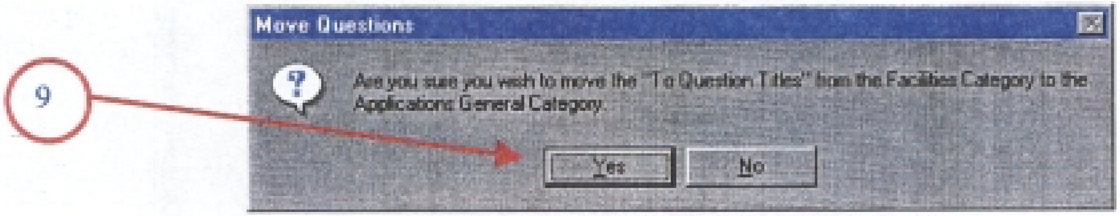
- □ AC 16 - Door Hinges
- □ AC 17 - Alarmed and Secure Wo
- □ AC 18 - Well Lighted and Lockec
- □ AC 19 - Separation of Areas from
- □ ADMIN 4 - Furniture and Supplie:
- □ COMPL 10 - Access to Handicap
- □ COMPL 11 - Environmental Haza

To Question Titles:

- □ ABCD
- □ ABCE

Question: NO

9. Click **Yes** if the moves are correct.

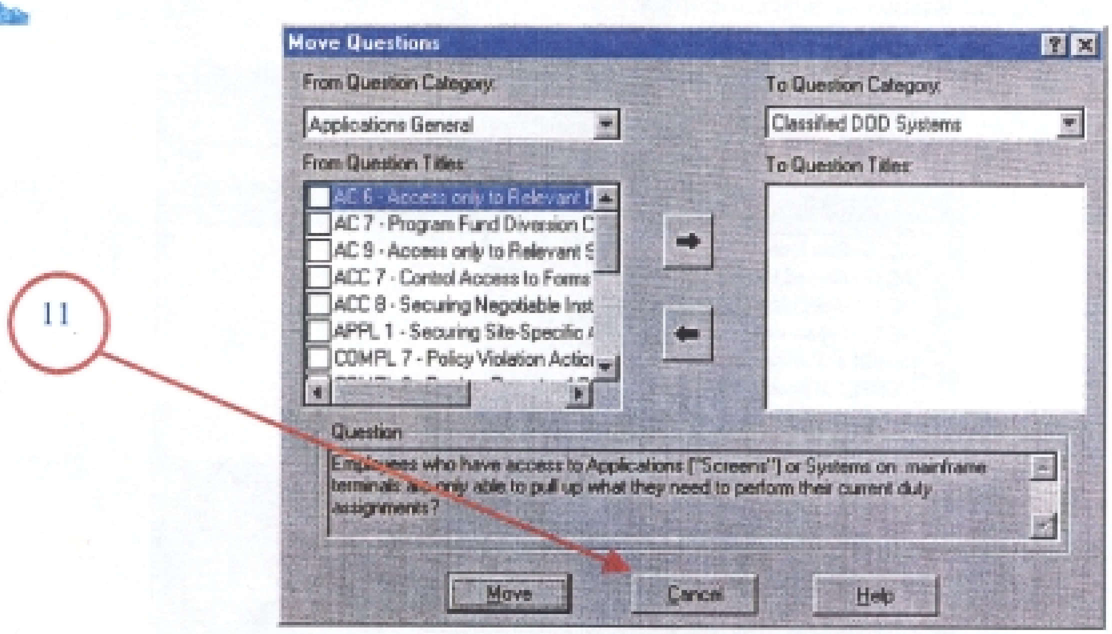


Move Questions

Are you sure you wish to move the "To Question Titles" from the Facilities Category to the Applications General Category.

10. Repeat steps 4 to 9 for each additional question category.

11. Select **Cancel** after moving all questions. RiskWatch returns to the Question Data dialog box.



From Question Category: Applications General

To Question Category: Classified DOD Systems

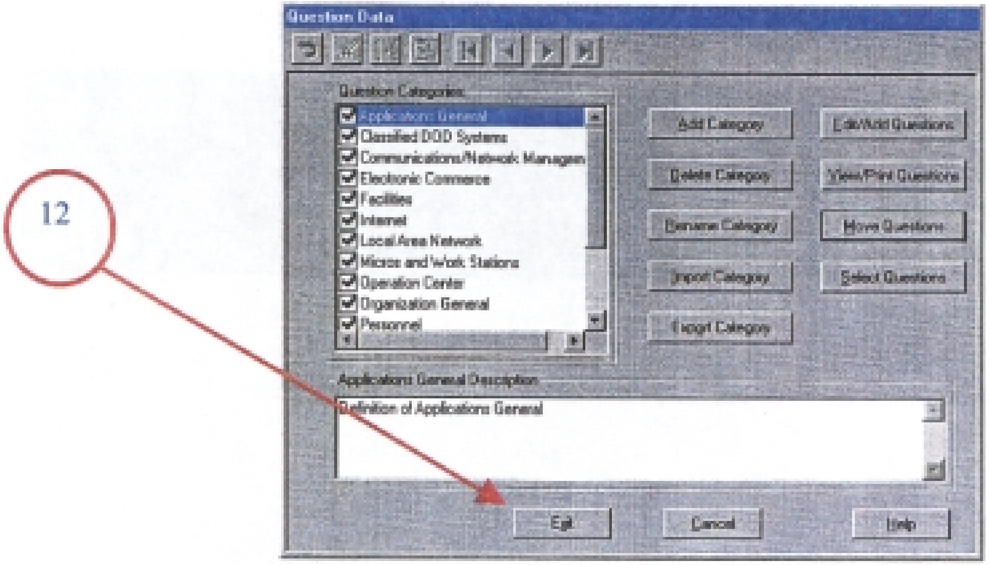
From Question Titles:

- □ AC 6 - Access only to Relevant I
- □ AC 7 - Program Fund Diversion C
- □ AC 9 - Access only to Relevant S
- □ ACC 7 - Control Access to Forms
- □ ACC 8 - Securing Negotiable Inst
- □ APPL 1 - Securing Site-Specific A
- □ COMPL 7 - Policy Violation Actio

To Question Titles:

Question: Employees who have access to Applications ["Screens"] or Systems on mainframe terminals are only able to pull up what they need to perform their current duty assignments?

12. Click **Exit** to return to the Question Phase tab.



Question Categories:

- ☑ Applications General
- ☑ Classified DOD Systems
- ☑ Communications/Network Managem
- ☑ Electronic Commerce
- ☑ Facilities
- ☑ Internet
- ☑ Local Area Network
- ☑ Micros and Work Stations
- ☑ Operation Center
- ☑ Organization General
- ☑ Personnel

Applications General Description: Definition of Applications General

13. **File, Save.**

Delete Individual Question

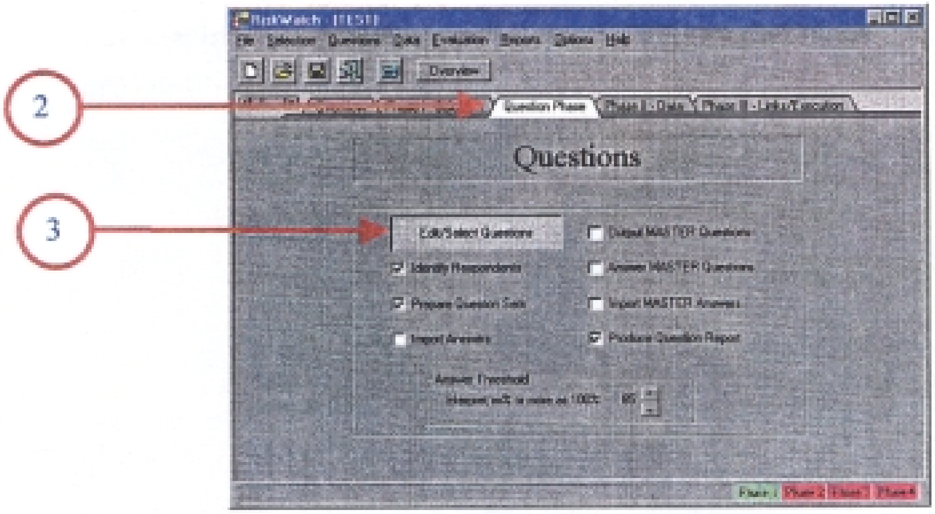
OPTIONAL

Deleting questions removes questions that do not apply to agency or business function.

WARNING
Deleted question cannot be recovered. If it is determined later that the question is needed, it will have to be imported from another review, the saved question database, or reenter it as a new question.

Step by step instructions: Deleting individual questions.

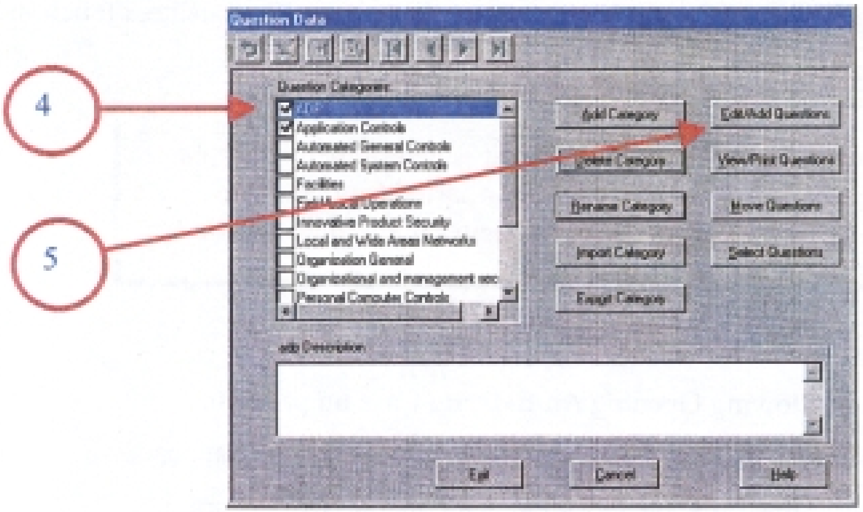
1. **Open** RiskWatch following Opening An Existing Case on page 40.
2. · Select **Question Phase** tab, the **Edit/Select Question** dialog box appears.
3. Select **Edit/Select Questions**, the Question Data dialog box appears.



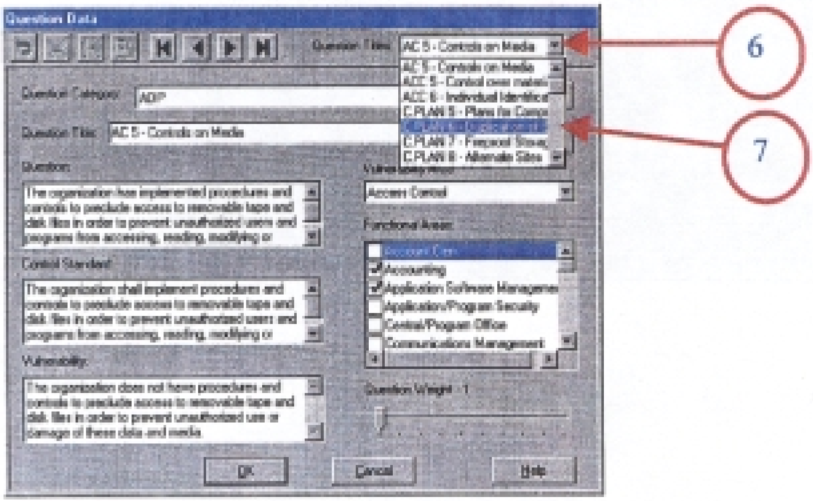
☑ Identify Respondents
☑ Prepare Question Sets
□ Import Answers
□ Output MASTER Questions
□ Answer MASTER Questions
□ Import MASTER Answers
☑ Produce Question Report

Answer Threshold
Interpret x% or more as 100%: 85

4. Highlight the **Question Category** in which the question is located.
5. Select **Edit/Add Questions**, a different Question Data dialog box appears.



6. Select the question using the pull-down triangle in the **Question Titles** box.
7. Find the Question needs to be deleted and highlight it. RiskWatch displays the Question Data.


6
7
Question Data
Question Titles
AC 5 - Controls on Media
ACC 5 - Control over mater
ACC 6 - Individual Identifica
C.PLAN 5 - Plans for Cont
C.PLAN 7 - Fireproof Storag
C.PLAN 8 - Alternate Sites
Functional Areas:
□ Account Exec
☑ Accounting
☑ Application Software Manageme
□ Application/Program Security
□ Central/Program Office
□ Communications Management
OK
Cancel
Help

Question Category: ADP

Question Title: AC 5 - Controls on Media

Question: The organization has implemented procedures and controls to preclude access to removable tape and disk files in order to prevent unauthorized users and programs from accessing, reading, modifying or

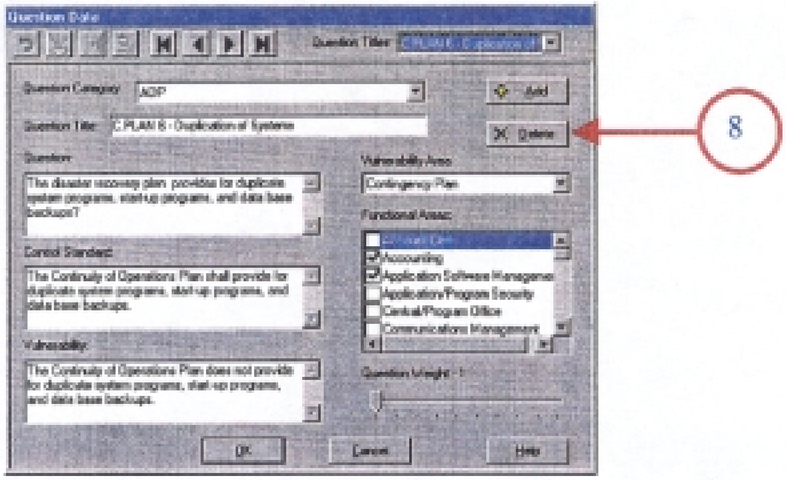
Control Standard: The organization shall implement procedures and controls to preclude access to removable tape and disk files in order to prevent unauthorized users and programs from accessing, reading, modifying or

Vulnerability: The organization does not have procedures and controls to preclude access to removable tape and disk files in order to prevent unauthorized use or damage of these data and media.

Vulnerability Area: Access Control

Question Weight - 1

8. Select **Delete**.



Question Titles: C.PLAN 6 - Duplication of

Question Category: ADP

Question Title: C.PLAN 6 - Duplication of Systems

Question:
The disaster recovery plan provides for duplicate system programs, start-up programs, and data base backups?

Control Standard:
The Continuity of Operations Plan shall provide for duplicate system programs, start-up programs, and data base backups.

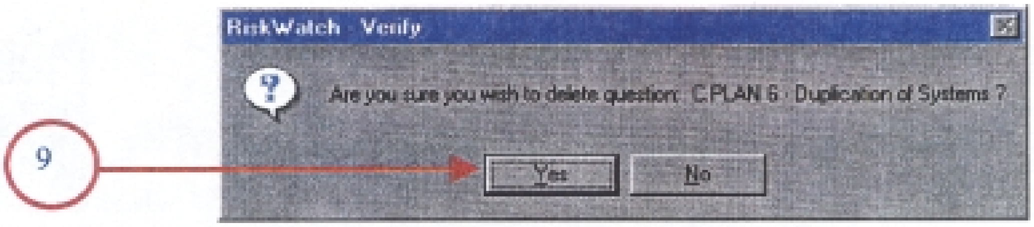
Vulnerability:
The Continuity of Operations Plan does not provide for duplicate system programs, start-up programs, and data base backups.

Vulnerability Area: Contingency Plan

Functional Areas:
- □ [illegible]
- ☑ Accounting
- ☑ Application Software Manageme
- □ Application/Program Security
- □ Central/Program Office
- □ Communications Management

Question Weight - 1

9. A **RiskWatch – Verify** dialog box appears and asks, "Are you sure you wish to delete question?" Select **Yes** if sure. This returns to the Question Data dialog box and deletes the question.



Are you sure you wish to delete question: C.PLAN 6 - Duplication of Systems ?

10. Repeat steps 5 to 9 until all needed questions have been deleted.

11. Click **O.K.,** returns to the Question Data dialog box.

12. Click **Exit,** returns to the Question Phase tab.

13. **File, Save.**

This concludes the Questions Phase How To Reference Guide.

This page left blank intentionally.

GLOSSARY

This glossary explains or defines terms used in the User's Guide or by RiskWatch. However, it does not include the categories definitions used by RiskWatch. Refer to Appendix C for the category definitions.

TERM	MEANING
AFE	See Annual Frequency Estimate
ALE	See Annual Loss Expectancy
Annual Frequency Estimate (AFE)	An annual estimated frequency of a threat's occurrence. Generally based on historical data and specific to a given environment, system, or geographic location.
Annual Loss Expectancy (ALE)	The sum of the Single Loss Expectancies (SLE) for all assets-loss combinations associated specific threat multiplied by the Annual Frequency Estimate (AFE).
Annual Maintenance Cost	The cost associated with the upkeep of a safeguard. May include one or more of the following: upgrade fees, labor, vendor/contract cost, data center cost, usage fees, etc.
Answer Threshold	A percentage used in the RiskWatch Question Phase to measure compliance. RiskWatch's default answer threshold is 85 percent, but the user has the ability to change it from 0-100. RiskWatch considers question responses below the answer threshold as non-compliant.
Asset Categories	RiskWatch has 21 asset categories from which the user may select and input individual asset data.
Assets	The tangible resources necessary for a system, function, or agency to perform its normal day-to-day operations or critical business functions. Examples include hardware, software, facilities, cash, data, and personnel.
Business Function	A discrete process or activity that results in a product or service that may or may not be associated with a specific system. Examples of UI business functions include benefit determinations, benefit payments, cashiering, tax audits, quality control, etc. Refer to UIPL 34-87 for a complete listing of UI business functions.
Confidentiality Cost for the asset (usually a data set)	Cost associated with the potential loss when restricted data is disclosed to an inappropriate source.

TERM	MEANING
Constant Detection (or Auditing) Cost for the Asset	The constant or fixed cost of ensuring that an asset is protected from unauthorized or unintentional modification. Included in this cost are purchase price and the hourly staff to monitor the system. Examples The constant cost of virus detection software, the cost of reviewing system logs, the cost of installing and operating proxy servers or firewalls to detect unauthorized access attempts, the cost of claimant fraud detection activities, etc.
Contingency Plan	A plan that, in case of disaster, identifies procedures, documentation, and resource schedules to be used in providing continued operating capability and support to all critical mission components.
Control Standard	A Control Standard should quote a policy, a procedure, a security precaution, or a commonly accepted business practice, etc. For Example "Passwords must be changed every 90 days."
Cost Effective Safeguard	A safeguard that results in a reduction in ALE greater than the safeguard's implementation and maintenance cost over the lifetime of the safeguard.
Cost per hour of unavailability of the asset measured to include consequent unavailability of all other dependent assets	The cost resulting from a delay or denial of service or productivity due to a realized threat to an asset. This cost includes the cost of downstream assets that also become unavailable.
Cost-Benefit Analysis Report	A report that analyzes the expected ALE reduction using the benefits and costs (implementation and maintenance) over the safeguard's lifetime.
Data Sensitivity Level	A field used under Organization Parameters in Phase I that indicates the level of the data's sensitivity or confidentiality. There are four levels suitable to the SESAs: Confidential, For Official Use Only, Not Applicable, or Privacy Act. Generally, "Privacy Act" is the level most appropriate for UI-related risk analyses.
Degree of Seriousness (SE)	The degree of loss to an asset that results from a realized threat. For the Delay/Denial Loss Category, RiskWatch measures the SE in hours; for all other loss categories, RiskWatch measures the SE as a percentage of the asset ranging from .0001 to 1.000. RiskWatch uses the SE to calculate the Single Loss Expectancy (SLE).
DOL	U.S. Department Of Labor
Downtime Before Serious Consequences	The number of hours an organization can go without the business function or system before experiencing serious consequences (i.e., losses).
FTE	See Full Time Equivalent (Users).

TERM	MEANING
Full-time Equivalent (FTE) Users	The number of employees employed in the business function under analysis or the number of employees who use a specific system
Functional Areas	The various position that personnel hold within an agency. RiskWatch links Functional Areas to questions to develop questions sets used to assess vulnerability in the Question Phase. RiskWatch uses 30 functional areas and allows the user to create new ones or modify existing ones
Implementation Cost	The cost associated with purchasing and installing a safeguard, which may include purchase price of the safeguard, shipping, sales tax, labor, set-up costs, etc.
Incident	A RiskWatch term used to describe the relationship between a threat, an asset, and a loss. For example, the "linking" relationship associated with Air-conditioning Failure (the Threat), Hardware (the Asset Category), and Delay Denial (the Loss Category). RiskWatch establishes default relationships that the user verifies.
Incident Class	The term used by RiskWatch to describe the relationship between an asset and a loss.
Intangible Losses	Losses incurred from embarrassment and loss of credibility.
LAFE	See Local Annual Frequency Estimate
Lifetime (in years)	The anticipated life expectancy of a safeguard, measured in years.
Linking Relationships	A "behind-the-scenes" function performed by RiskWatch to establish default relationships between assets, threats, losses, and vulnerability areas in Phase III.
Local Annual Frequency Estimate (LAFE)	The same as an AFE, but specifically tied to the "local" environment, system, business function, or geographic location. The user establishes the LAFE in Phase II of RiskWatch.
Loss	A loss results from the realization of a threat that causes a decrease in the amount, magnitude, or degree of an asset's value, integrity, availability, or confidentiality.
Loss Categories	RiskWatch provides six categories of loss. (See Loss.)
Make-up Cost	The labor cost associated with processing backlogs or resuming normal day-to-day operations after an asset is replaced, recovered, etc. This cost is related to the Cost per Hour of Unavailability of the Asset and the Delay/Denial Loss Category.
Operational Cost	The labor cost associated with ongoing, normal day-to-day operations that are lost when an asset becomes unavailable. This cost is related to the Cost per Hour of Unavailability of the Asset and the Delay/Denial Loss Category.

TERM	MEANING
Organization Parameters	A set of facts used by RiskWatch in Phase II that define scope or boundaries of an agency or subject and its environment and assets.
Percentage of mission dependent on this asset	The percentage of the business function (i.e., mission) that relies on the asset in order to perform its day-to-day operations.
Question Set	A term used to describe the combination of a Control Statement, Question Statement, and Vulnerability Statement. Also used to describe a set of questions prepared for a specific Respondent either in paper copy, on disk, from a LAN shared drive, etc.
Question Statement	A statement used to query respondents concerning the degree of compliance to a Control Standard. In RiskWatch, Question Statements are not phrased as questions, but phrased as a positive affirmation to the Control Standard. EXAMPLE: "Passwords are changed every 90 days"
Question Weight	A value between 1 and 10 used to indicate the importance or significance of a question. The higher the weight, the more important or significant the questions. RiskWatch's default weight is one (1).
Replacement Cost for the asset	The cost to replace a lost asset. Generally, this includes the purchase price, shipping, sales tax, installation, etc.
Respondent	An individual selected for his/her knowledge, experience, and ability to respond to a Question Set. A Respondent is associated with one or more Functional Areas.
Risk	Exposure to a danger or hazard.
Risk Analysis	An analytical method used to measure an agency's level of risk that addresses four areas: valuation of assets, measurement of vulnerability, impact of threats, and effectiveness of safeguards.
SAFE	See Standard Annual Frequency Estimate
Safeguard Evaluation	An automatic function performed by RiskWatch that analyzes the potential effectiveness of safeguards.
Safeguard	The technical, procedural, and environmental controls that protect an agency's assets from loss by eliminating or minimizing the vulnerabilities that lead to a realized threat. May also be referred to as a control.
SE	See Degree of Seriousness
Security Mode	The level of security at which a system operates. RiskWatch provides six options; however, users are advised to use Not Applicable as this appears to relate Department of Defense systems only.

TERM	MEANING
Sensitivity Level	Generally, for any risk analysis associated with UI, the writers of this manual suggests the analyst select "Privacy Act".
SESA	State Employment Security Agency
Single Loss Estimate (SLE)	The sum of the Single Loss Expectancies for all assets attributed to a specific realized threat.
SLE	See Single Loss Estimate
Standard Annual Frequency Estimate (SAFE)	The same as an AFE, but based on a fixed national average developed by RiskWatch that the user cannot modify. The SAFE is the default value.
Threat Agent:	Any person or thing, which acts, or has the power to act, to cause, carry out, transmit or support a threat.
Threat	Any potential human or natural event, process, act, or substance that results in a loss to an assets availability, integrity, or confidentiality. Threats are always present.
Threats Frequencies	Refer to AFE, LAFE, or SAFE.
Time to Replace Minimal Functional Support	The number of hours required by an agency to resume minimal/essential operations for a business function or system ***OR*** the number of hours in which the agency is required or mandated to be operational by state or agency requirements.
Total Potential Cost to the Enterprise arising from this asset becoming contaminated.	The cost associated with an asset, generally a database, system software, or application, that becomes corrupted due to unauthorized modification, such as through a virus or sabotage.
UINRAP	Unemployment Insurance National Risk Analysis Project.
Value of the Mission for the Enterprise, Per Annum	
Vulnerability	The result of weaknesses in an agency's line of defense against threats, such as inadequate or non-existent controls (i.e., safeguards). These weaknesses provide an opportunity for loss to an asset or a set of assets when a threat occurs.
Vulnerability Area	RiskWatch has 24 predefined Vulnerability Areas from which the analyst may select in Phase III.
Vulnerability Statement	A statement that shows a negative reflection of a Control Standard. For example, "Passwords are not changed every 90 days" is a negative reflection of the Control Standard "Passwords are changed every 90 days."
What Ifs Scenarios	An optional feature in Phase III that produces reports listing all the threats that impact a selected safeguard and compares the ALE with and without the safeguard.

This page left blank intentionally.

Appendix A Supplemental Data

Worksheet, Tables, and RiskWatch Screen Prints

The Project Team has provided tables, worksheets and RiskWatch screen prints as tools to use during Ideas For Collecting and Organizing Data on page 15.

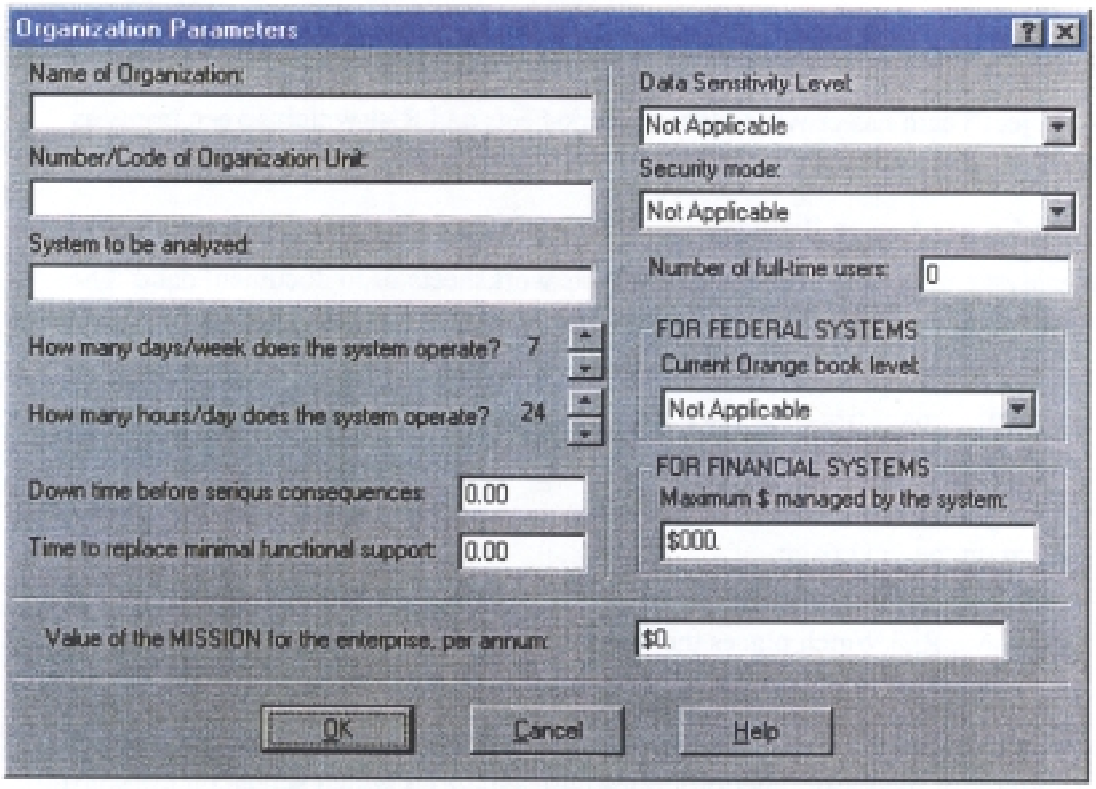
How to Create Screen Prints

The analyst can make screen prints to use as worksheets or to document data. The procedure for creating screen prints is as follows:

1. Open the case, if it is closed. The **Overview** tab appears.
2. Open WordPad, WordPerfect 6.0 or above, or Microsoft Word and minimize the screen and return to RiskWatch.
3. Identify the screen needing to be copied, such as the **Organization Parameters** screen on the next page.
4. First press and hold the **Alt** key, then press the **Print Screen** key. After releasing both keys, RiskWatch places the screen print on the clipboard.
5. Maximize the word processing application.
6. Press and hold the **Ctrl** key, then press the **"v"** key, and then release (i.e., the shortcut for the Paste function). This pastes the RiskWatch screen on the word processing document. The analyst can size and print this page to use as a data collection tool.

The following page provides a blank copy of the Organization Parameters screen print for use as a worksheet.

Form 1 Organization Parameter Worksheet



Organization Parameters

Name of Organization:

Number/Code of Organization Unit:

System to be analyzed:

How many days/week does the system operate? 7

How many hours/day does the system operate? 24

Down time before serious consequences: 0.00

Time to replace minimal functional support: 0.00

Data Sensitivity Level: Not Applicable

Security mode: Not Applicable

Number of full-time users: 0

FOR FEDERAL SYSTEMS

Current Orange book level: Not Applicable

FOR FINANCIAL SYSTEMS

Maximum $ managed by the system: $000.

Value of the MISSION for the enterprise, per annum: $0.

Asset Data

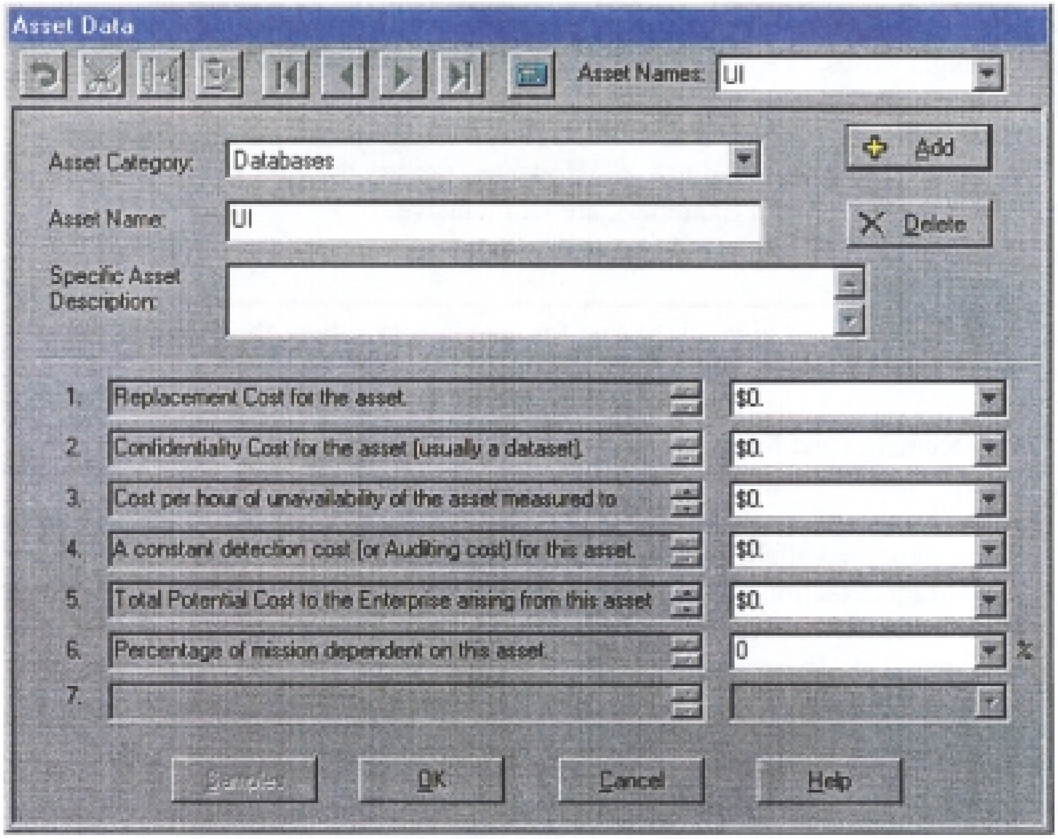
Use the either Form 2 or Form 3 to document the asset data prior to entering it into RiskWatch. Table 4 Asset Category Data Elements indicates which data elements each asset category uses. Table 5, Table 6, and Table 7 provide detailed information on Replacement, Confidentiality, and per Hour of Unavailability costs. These three tables include the asset category definition, UI related examples, and suggestions for where/how to develop the needed values. However, neither the RiskWatch's definitions nor the UI Related Examples, are all inclusive.

Since Form 2 does not give all the text for the six cost values, they are presented below.

1. Replacement Cost for the asset.
2. Confidentiality Cost for the asset (usually a data set).
3. Cost per hour of unavailability of the asset measured to include consequent unavailability of all other dependent assets.
4. A constant detection cost (or Auditing cost) for this asset.
5. Total Potential Cost to the Enterprise arising from this asset becoming contaminated. In general, this cost is in no way related to the basic costs of the asset.
6. Percentage of mission dependent on this asset.

For assistance on the "what, where, and how's" of developing these cost figures, refer to Overview Of The RiskWatch® Process on page 9.

Form 2 Asset Worksheet



Asset Names: UI

Asset Category: Databases

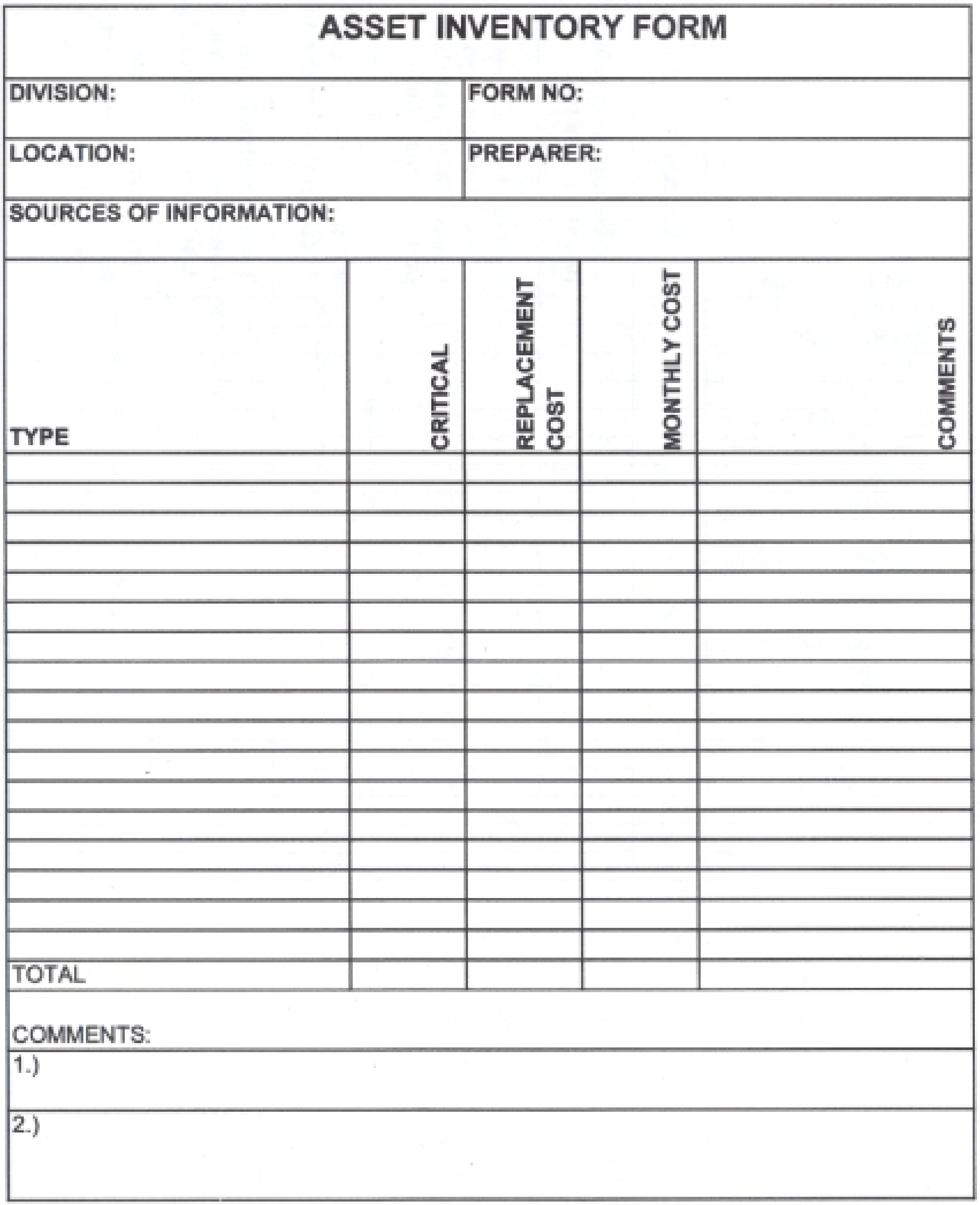
Asset Name: UI

Specific Asset Description:

1.	Replacement Cost for the asset.	$0.
2.	Confidentiality Cost for the asset (usually a dataset).	$0.
3.	Cost per hour of unavailability of the asset measured to	$0.
4.	A constant detection cost (or Auditing cost) for this asset.	$0.
5.	Total Potential Cost to the Enterprise arising from this asset	$0.
6.	Percentage of mission dependent on this asset.	0 %
7.		

Form 3 Asset Inventory Form

Use the form below to document inventory or use this form as a sample to develop a customized form for the agency or business functions.



ASSET INVENTORY FORM					
DIVISION:		**FORM NO:**			
LOCATION:		**PREPARER:**			
SOURCES OF INFORMATION:					
TYPE	**CRITICAL**	**REPLACEMENT COST**	**MONTHLY COST**	**COMMENTS**	
TOTAL					
COMMENTS:					
1.)					
2.)					

Asset Categories	Replacement Co	Confidentiality c (usually a data s	Cost per hour of of the Asset meas consequent unav other dependent	A Constant Dete Auditing) Cost fo	Total Potential C Enterprise arisin Asset becoming	Percentage of Mi dependent on thi
Accounts Payable	X		X	X	X	X
Accounts Receivable	X		X	X	X	X
Applications	X		X	X	X	X
Cash Accounts	X		X	X	X	
Communications Hardware	X		X			X
Communications Software	X		X	X	X	X
Data Bases	X	X	X	X	X	X
Documentation	X		X			
Facilities	X		X			X
Fire Detection/Suppression	X		X			
Hardware	X		X			X
Intangibles	X					
Negotiable Instruments	X		X	X	X	
Office Equipment	X		X			
Personnel	X	X	X			X
Procedures	X		X			
Security	X		X			
Supplies & Consumables	X		X			
Support Systems	X		X			X
System Software	X		X	X	X	X
Utilities	X		X			

Asset Costing Tables

As stated in Section 3, RiskWatch requires the analyst to input as many as six (6) data elements per asset, depending on the asset category. For each data element, Section 3 provides, as appropriate, a translation of the data element terminology and/or suggestions on how to develop the cost. The three tables below provide

Table 5 Replacement Cost

REPLACEMENT COST		
Asset Category	**UI Related Examples**	**Suggestions for Replacement Cost Values**
ACCOUNTS PAYABLE - Includes all money, including notes and loans, which the organization owes to any other entity.	◆ Moneys due to employers, claimants, and vendors	Use the balance as of a specific date
ACCOUNTS RECEIVABLE - Refers to all the money owed to the organization, including all outstanding invoices; all money billed, but not yet collected; and all long-term loans.	◆ Moneys owed to the agency from employers and claimants ◆ Administrative funding from DOL	Use the balance as of a specific date. Amount allocated annually to the business function under analysis.
APPLICATIONS - Refers to special function programs usually developed for the system being analyzed such as inventory control, payroll, etc.	◆ Benefits ◆ Overpayment ◆ Tax ◆ Job Service ◆ Mainframe Applications ◆ Client-Server Applications ◆ SUN Sparc Applications	With back up, use a reasonable figure, generally the labor cost to restore the application. For Example Multiply the # of staff required x the hourly pay of the individual(s) to restore the backup. Without back up, the cost to rewrite code on a cost per line or the cost per hour basis.
CASH ACCOUNTS – Refers to all the cash possessed by the organization, including petty cash.	◆ UI Trust Fund ◆ Petty Cash	Use the balance as of a specific date

REPLACEMENT COST		
Asset Category	**UI Related Examples**	**Suggestions for Replacement Cost Values**
COMMUNICATIONS HARDWARE – Communications assets include modems, multiplexers, cabling, communications boards, encryption devices, satellite dishes, antennas, and applicable software.	◆ Modems ◆ Telephones ◆ Fax	Use the current purchase price of the item to replace it. Include labor, set up costs (cabling, site preparation), tax, and shipping. If a current purchase price is unavailable, use the actual purchase price and adjust for inflation or changes in industry pricing (i.e., decrease in computer costs) Leased equipment can be calculated as if owned
COMMUNICATIONS/ NETWORK SOFTWARE - No definition available.	◆ ProCom ◆ Extra ◆ Browser software ◆ Phone company software	Use the current purchase price of the item to replace it. (Same as Communications Hardware.)
DATA BASES - Refers to any data file used by any payroll, client eligibility programs, and inventory listings, etc.	◆ Employer Record ◆ Claimant Address Records ◆ Claimant Claim Record ◆ Wage Records	With back up, use a reasonable figure, generally the labor cost to restore the application. For Example Multiply the # of staff required x the hourly pay of the individual(s). Without back up, cost to re-collect data, such as contacting employers to resubmit wage records. Also, the cost to re-enter data once collected.

REPLACEMENT COST

Asset Category	UI Related Examples	Suggestions for Replacement Cost Values
DOCUMENTATION - Documentation refers to both manuals and hard copies of listings of programs and operating procedures used by the system.	◆ Completed UI Claims ◆ System documentation (flowcharts, etc.) ◆ Invoices ◆ Travel vouchers ◆ Cancelled checks ◆ Employer reports ◆ Wage reports ◆ Incident reports ◆ Federal reports ◆ Business function specific documents ◆ Back-up documentation ◆ Microfilm/fiche ◆ CD ROM, Tape, Disk media on which data is image/stored	The labor cost to recreate the documentation; cost of printing, cost of media (paper, CD-ROM, tape, disk, etc.). Can determine labor by the hour or by minutes per unit (MPU) or use contractor price.
FACILITIES - Facilities includes buildings as well as shared facilities such as coffee shops, employee lunch rooms, restrooms, etc	◆ Field offices ◆ Central office or headquarters ◆ Call centers ◆ One-Stop sites	Use either the cost to replace the entire facility or proportion to the amount of space the business function occupies in the facility. Can use current market estimates per square foot for rebuilding a comparable facility. For leased facilities, calculated on the cost per square foot to lease a replacement site.
FIRE DETECTION AND SUPPRESSION SYSTEMS - Fire Detection and Suppression assets include smoke and alarms, fire alarms, humidity sensors, and fire suppression systems consisting of combinations of CO2, Water, or chemical foam.		Use either the cost to replace the entire system or proportion to the amount of space the business function occupies in the facility. Can use current market estimates for replacing a system in a comparable facility.
HARDWARE - This category includes Central Processing Units (CPUs), printers, diskettes, tapes, controllers, mainframes, minis, micros, as well as "dumb" terminals.	◆ Imaging systems ◆ Scanners ◆ Mainframe servers ◆ PCs (workstations) ◆ Printers ◆ Check printers ◆ LAN Servers ◆ Routers, hubs ◆ Dumb terminals ◆ Signature plates	Use Use the current purchase price of the item to replace it. (Same as Communications Hardware.) Leased equipment can be calculated as if owned.

REPLACEMENT COST		
Asset Category	**UI Related Examples**	**Suggestions for Replacement Cost Values**
INTANGIBLES (REPUTATION) - This category includes considerations of a non-material nature such as the reputation of the organization and its credibility.	◆ UI/Agency Reputation ◆ Public Trust/Good Will	Can use a percentage of: ◆ Agency's mission. ◆ Business function's total assets. ◆ Total losses for the business function. Use best judgement to determine the percentage appropriate for the agency; consider input from legal, fiscal, and public relations experts.
NEGOTIABLE INSTRUMENTS - Includes all stock certificates, bonds, food stamps, coupons, travelers' cheques, gift certificates and any other item that could be exchanged for cash.	◆ Checks ◆ Credit cards ◆ Check stock ◆ Travel/transportation vouchers	Cost to reprint or replace stock, voucher, etc.
OFFICE EQUIPMENT - Includes office desks, tables chairs, filing cabinets, lamps, sofas, carpets, and any other type of office furniture.		Use the current purchase price of the item to replace it. (Same as Communications Hardware.) Leased equipment can be calculated as if owned. Can also use a cost per person or workstation.
PERSONNEL - Includes all support people of the organization including administrators, systems support people, operators, users, and any person who has anything to do with the system.	◆ Benefit function personnel ◆ IT personnel ◆ Administrative Services personnel (human resources, procurement, facility, etc.) ◆ Tax function personnel ◆ Management	Include personnel directly and indirectly involved with the business function; proportion time as necessary. Include cost to recruit, interview, and train replacement staff. Include salary and benefit costs.
PROCEDURES - This category includes the operating procedures of the system, including procedures for hiring, administrative procedures, and procedures for emergency response.	◆ Contingency Plans ◆ Evacuation Procedures ◆ Business function procedure manuals ◆ Administrative manuals ◆ Software manuals	See Documentation above.

REPLACEMENT COST		
Asset Category	**UI Related Examples**	**Suggestions for Replacement Cost Values**
SECURITY SYSTEMS - Includes motion detectors, video cameras, access control systems, card key systems, locks, safes, security software (such as TOP SECRET), password programs, fences, and encryption devices.	◆ Security systems ◆ Locking devices ◆ Safes ◆ Security guard salaries ◆ Bullet-proof glass ◆ Security/safety training ◆ RACF/ACF2 ◆ Authentication software ◆ Internal security staff ◆ Firewalls/proxy servers ◆ Single Sign-On software ◆ Hot site agreements ◆ Back-up media & storage	Refer to Hardware or System Software for determining replacement costs.
SUPPLIES AND CONSUMABLES - Includes office supplies such as paper, ribbons, tapes, disks, folders, pens, pencils, etc.		See Hardware above. Can also use a standard cost "per person".
SUPPORT SYSTEMS - Includes air conditioning systems, heating systems, humidifying systems, fuel systems, cooling systems for machinery and grounding systems.	◆ Back-up generators for check printing facilities or mainframe.	Consider including this under "Facilities".
SYSTEM SOFTWARE - Includes job language programs and all operating system programs, such as DOS, CPM, UNIX, OS, GCOS, VMS, etc.	◆ Network operating systems ◆ Support software (Windows 95, Windows NT, Novell, O/S2, etc.) ◆ Data base software (Oracle, DB2, etc.)	Use the current purchase price of the item to replace it. (Same as Communications Hardware.)
UTILITIES - Includes electrical power, telephone systems, natural gas, water and fuel.		Consider including this under "Facilities" or the analyst can use the cost to install the utility and any hook-up fees.

Table 6 Confidentiality Cost for the Asset (Disclosure)

DISCLOSURE		
Asset Category	**UI Related Examples**	**Suggestions for Confidentiality Cost Values**
DATABASES - Refers to any data file used by any payroll, client eligibility programs, and inventory listings, etc.	◆ Employer Record ◆ Claimant Address Records ◆ Claimant Claim Record ◆ Wage Records	RiskWatch suggests using a cost $5,000 per record for the disclosure of a Privacy Act record or $1,000 for official use only records. $5,000 is an industry standard; $1,000 is the Department of Navy standard. Since it is unlikely that all records would be disclosed, use a percentage for calculating the loss. RiskWatch recommends 5%. Example $5,000 (cost per record disclosed) X 10,000 records = $50 million (total potential disclosure cost) 5% (estimate of actual records disclosed) X $50 million (total potential disclosure cost) = $2.5 million (confidentiality cost).
DOCUMENTATION - Refers to both manuals and hard copies of listings of programs and operating procedures used by the system.	◆ Completed UI Claims ◆ System documentation (flowcharts, etc.) ◆ Invoices ◆ Travel vouchers ◆ Cancelled checks ◆ Employer reports ◆ Wage reports ◆ Incident reports ◆ Federal reports ◆ Business function specific documents ◆ Back-up documentation ◆ Microfilm/fiche ◆ CD ROM, Tape, Disk media on which data is image/stored	Use the same method as above, but on a per document basis.

DISCLOSURE		
Asset Category	**UI Related Examples**	**Suggestions for Confidentiality Cost Values**
PERSONNEL - Includes all support people of the organization including administrators, systems support people, operators, users, and any person who has anything to do with the system.		Use $5,000 per employee for loss following the method used for Databases.
PROCEDURES - Includes the operating procedures of the system, including procedures for hiring, administrative procedures, and procedures for emergency response.		Use the same method as above for "official use only" data (i.e., $1,000 per item), but on a per procedure basis.
SYSTEM SOFTWARE - Includes job language programs and all operating system programs, such as DOS, CPM, UNIX, OS, GCOS, VMS, etc.		Use the same method as above for "official use only" data (i.e., $1,000 per item), but on a per software license basis.

Table 7 Cost Per Hour of Unavailability of the Asset (Delay/Denial)

Delay/Denial		
Asset Category	**UI Related Examples**	**Suggestions for Delay/Denial Values**
ACCOUNTS PAYABLE - Includes all the money, iricluding notes and loans, which the organization owes to any other entity.	◆ Moneys due to employers, claimants, and vendors	Loss of interest charges or fees for late payments. Loss of potential discounts for vendors Make-up costs
ACCOUNTS RECEIVABLE - Refers to all the money owed to the organization, including all outstanding invoices; all money billed, but not yet collected; and all long term loans.	◆ Moneys owed to the agency from employers and claimants ◆ Administrative funding from DOL	Loss of Penalty and Interest (P & I) Loss of any interest received on money in fund Make-up costs
APPLICATIONS – Refers to special function programs usually developed for the system being analyzed such as inventory control, payroll, etc.	◆ Benefits ◆ Overpayment ◆ Tax ◆ Job Service ◆ Mainframe applications ◆ Client-Server applications ◆ SUN Sparc applications	Make-up costs Operational costs
CASH ACCOUNTS – Refers to all the cash possessed by the organization, including petty cash.	◆ UI Trust Fund ◆ Petty Cash	Loss of Penalty and Interest (P&I) Loss of any interest received on money in fund Make-up costs
COMMUNICATIONS HARDWARE - Communications assets include modems, multiplexers, cabling, communications boards, encryption devices, satellite dishes, antennas, and applicable software.	◆ Modems ◆ Telephones ◆ Fax	Operational costs Make-up costs Loss of ability to transfer funds via modem. (This may cause loss of interest; inability to pay benefits.) Inability to receive employer or claimant information via fax may affect timely decisions.
COMMUNICATIONS SOFTWARE - No definition available	◆ ProCom ◆ Extra ◆ Browser software ◆ Phone company software	See "Communications Hardware"
DATABASES – Refers to any data file used by any payroll, client eligibility programs, and inventory listings. etc.	◆ Employer Record ◆ Claimant Address Records ◆ Claimant Claim Record ◆ Wage Records	See "Applications"

Delay/Denial		
Asset Category	**UI Related Examples**	**Suggestions for Delay/Denial Values**
DOCUMENTATION - Refers to both manuals and hard copies of listings of programs and operating procedures used by the system.	◆ Completed UI Claims ◆ System documentation (flowcharts, etc.) ◆ Invoices ◆ Travel vouchers ◆ Cancelled checks ◆ Employer reports ◆ Wage reports ◆ Incident reports ◆ Federal reports ◆ Business function specific documents ◆ Back-up documentation ◆ Microfilm/fiche ◆ CD ROM, Tape, Disk media on which data is image/stored	Operational costs Make-up costs Any penalties for untimely reporting
FACILITIES - Facilities includes buildings as well as shared facilities such as coffee shops, employee lunch rooms, restrooms, etc	◆ Field offices ◆ Central office or headquarters ◆ Call centers ◆ One-Stop sites	Operational costs Make-up costs
FIRE DETECTION & SUPPRESSION – Fire Detection and Suppression assets include smoke and alarms, fire alarms, humidity sensors, and fire suppression systems consisting of combinations of CO2, Water, or chemical foam.		Loss of fire protection, possible loss of asset availability through damage or destruction. Operational and Make-up costs due to evacuation (false alarm, tornado, etc.)
HARDWARE – This category includes Central Processing Units (CPUs), printers, diskettes, tapes, controllers, mainframes, minis, micros, as well as "dumb" terminals.	◆ Imaging systems ◆ Scanners ◆ Mainframe servers ◆ PCs (workstations) ◆ Printers ◆ Check printers ◆ LAN Servers ◆ Routers, hubs ◆ Dumb terminals ◆ Signature plates	Operational costs Make-up costs

Delay/Denial		
Asset Category	**UI Related Examples**	**Suggestions for Delay/Denial Values**
NEGOTIABLE INSTRUMENTS - Includes all stock certificates, bonds, food stamps, coupons, travelers cheques, gift certificates and any other item which could be exchanged for cash.	◆ Checks ◆ Credit cards ◆ Check stock ◆ Travel/transportation vouchers	Operational costs Make-up costs
OFFICE EQUIPMENT - Includes office desks, tables chairs, filing cabinets, lamps, sofas, carpets, and any other type of office furniture.		Operational costs Make-up costs
PERSONNEL – Includes all support people of the organization including administrators, systems support people, operators, users, and any person who has anything to do with the system.	◆ Benefit function personnel ◆ IT personnel ◆ Administrative Services personnel (human resources, procurement, facility, etc.) ◆ Tax function personnel ◆ Management	Operational costs Make-up costs
PROCEDURES - Includes the operating procedures of the system, including procedures for hiring, administrative procedures, and procedures for emergency response.	◆ Contingency Plans ◆ Evacuation Procedures ◆ Business function procedure manuals ◆ Administrative manuals ◆ Software manuals	Operational costs Make-up costs
SECURITY – Includes motion detectors, video cameras, access control systems, card key systems, locks, safes, security software (such as TOP SECRET), password programs, fences, and encryption devices.	◆ Security systems ◆ Locking devices ◆ Safes ◆ Security guard salaries ◆ Bullet-proof glass ◆ Security/safety training ◆ RACF/ACF2 ◆ Authentication software ◆ Internal security staff ◆ Firewalls/proxy servers ◆ Single Sign-On software ◆ Hot site agreements ◆ Back-up media & storage	Operational costs Make-up costs
SUPPLIES AND CONSUMABLES - Includes office supplies such as paper, ribbons, tapes, disks, folders, pens, pencils, etc.		Operational costs Make-up costs

Delay/Denial		
Asset Category	**UI Related Examples**	**Suggestions for Delay/Denial Values**
SUPPORT SYSTEMS - Includes air conditioning systems, heating systems, humidifying systems, fuel systems, cooling systems for machinery and grounding systems.	◆ Back-up generators for check printing facilities or mainframe.	Operational costs Make-up costs
SYSTEM SOFTWARE - Includes job language programs and all operating system programs, such as DOS, CPM, UNIX, OS, GCOS, VMS, etc.	◆ Network operating systems ◆ Support software (Windows 95, Windows NT, Novell, O/S2, etc.) ◆ Data base software (Oracle, DB2, etc.)	Operational costs Make-up costs
UTILITIES – Includes electrical power, telephone systems, natural gas, water and fuel.		Operational costs Make-up costs

Local Annual Frequency Estimate (LAFE)

Table 8 provides the analyst some suggested sources for developing LAFE for each threat type Form 4 provides the default SAFE values used by RiskWatch. In the SESA LAFE column, indicate the LAFE used in the case and document the data source(s) used to develop the LAFE. For future reference, attach any supporting documentation to the form.

Table 8 Local Annual Frequency Sources

THREAT	SUGGESTED SOURCE(S)
Air Conditioning Failure	Maintenance, Building Oversight
Aircraft Accident	State Emergency Management Administration (SEMA)
Biological Contamination/ Chemical Spill	Local/SEMA
Blackmail/Bomb Threat	Personnel responsible for incidents reports
Budget Loss	Controller Financial Officer
Cold, Frost, Snow	Local weather station, personnel overseeing annual leave
Communication Loss	Administrative Services Contractor providing communication service
Competition Pirating Key Personnel	Personnel Information Technology Officer
Data Destruction Data Disclosure Data Integrity Loss	UI Internal Security Information Technology Officer Disclosure Officer
Earthquakes	SEMA
Electromagnetic Interference Emanations	Information Technology
Errors, General/All	Through research, use best judgement Business function management
Fires: Catastrophic, Major, Minor, False Alarm	State and local Fire Marshall, Administrative services, Risk management
Flooding/Water Damage	SEMA, Maintenance or building oversight
Fraud/Embezzlement	UI Internal Security
Hardware Failure	Information Technology
Misuse Computer	UI Internal Security, Information Technology
Nuclear Mishaps	SEMA
Power Loss	Administrative services/maintenance Information Technology Network Administrator

THREAT	SUGGESTED SOURCE(S)
Resource Mismanagement	Human Resources
Sabotage	Internal Security SEMA Information Security Officer
Sinking Ground/ Storms/Hurricanes	SEMA
Substance Abuse	UI Internal Security Personnel Officer Payroll Officer
Theft of Assets Theft of Data	Inventory Control UI Internal Security (ETA 9000) Information Technology Financial Officer
Vandalism/Rioting	Local police UI Internal Security Safety Officer Financial Officer

Form 4 – Threat LAFE Worksheet

Threat	RiskWatch SAFE	SESA LAFE	Data Source(s)
Air Conditioning Failure	3.00		
Aircraft Accident	0.01		
Biological Contamination	0.05		
Blackmail	0.05		
Bomb Threats	2.00		
Budget Loss	0.50		
Chemical Spills	0.01		
Cold/Frost/Snow	5.00		
Communications Loss	100.00		
Competition	5.00		
Currency Fluctuation	4.00		
Data Destruction	20.00		
Data Disclosure	3.00		
Data Integrity Loss	3.00		
Earthquake	0.01		
Electromagnetic Interference	5.00		
Emanations	5.00		
Errors, General/All	150.00		
Fire, Catastrophic	0.01		
Fire, False Alarm	2.00		
Fire, Major	0.01		
Fire, Minor	0.01		
Flooding/Water Damage	0.01		
Fraud/Embezzlement	1.00		
Hardware Failure	70.00		
Inflation	0.50		
Misuse: Computer	5.00		
Nuclear Mishap	0.01		
Pirating Key Personnel	1.00		
Power Loss	12.00		
Resource Mismanagement	5.00		
Sabotage	0.10		
Sinking Ground	0.01		
Storms/Hurricanes	0.10		
Substance Abuse	4.00		
Theft of Assets	5.00		
Theft of Data	5.00		
Vandalism/Rioting	1.00		

Safeguard Details

Use either Form 5 or Form 6 to develop safeguard data. Form 5 documents all the safeguards related to a single safeguard category. Form 6 documents the totals for all the safeguard categories. Form 6 also provides RiskWatch's default Lifetime values.

Form 5 Safeguard Worksheet by Category

SAFEGUARD CATEGORY:		
Safeguard #1		
Description:	Implementation Cost: $	Lifetime (in years):
Vulnerability/Threat Addressed:	Annual Maintenance: $	% Implemented:
Data Source:		
Safeguard #2		
Safeguard Description:	Implementation Cost: $	Lifetime (in years):
Vulnerability/Threat Addressed:	Annual Maintenance: $	% Implemented:
Data Source:		
Safeguard #3		
Safeguard Description:	Implementation Cost: $	Lifetime (in years):
Vulnerability/Threat Addressed:	Annual Maintenance: $	% Implemented:
Data Source:		
Safeguard #4		
Safeguard Description:	Implementation Cost: $	Lifetime (in years):
Vulnerability/Threat Addressed:	Annual Maintenance: $	% Implemented:
Data Source:		
Totals for the Category		
Safeguard Description:	Implementation Cost: $	Lifetime (in years):
Vulnerability/Threat Addressed:	Annual Maintenance: $	% Implemented:

Form 6 Safeguard Data Worksheet

Safeguard Category	Implementation Cost	Annual Maintenance Cost	Percentage Implemented	RiskWatch Default Lifetime	SESA Lifetime	Data Source
Physical Access Control				3		
Application Controls				3		
Audit Trails				5		
Classification Markings				3		
Contingency Plan				2		
Contract Specifications				1		
Data Encryption				5		
Detection System				3		
Documentation				3		
Electrical Power				10		
Emergency Response				3		
File/Program Control				5		
Fire Suppression				5		
Grounding System				3		
Insurance/ Bond				1		
Life Cycle Management				1		
Material Segregation				3		
Monitor System				3		
New Construction				50		
Operating Procedures				3		
Office of Primary Responsibility for Each System				1		
Organizational Structure				1		
Passwords/ Authentication				5		
Personnel Clearances				1		
Personnel Control				3		
Preventative Maintenance				1		
Property Management				3		
Quality Assurance				5		
Redundant Power				20		

Safeguard Category	Implementation Cost	Annual Maintenance Cost	Percentage Implemented	RiskWatch Default Lifetime	SESA Lifetime	Data Source
Review of Sensitive Applications				3		
Risk Analysis				3		
Security Classification				1		
Security Plan				3		
Security Policy				3		
Security Staff				3		
Safeguard Test & Evaluation				3		
System Validation				2		
Technical Surveillance				3		
Tempest Survey				5		
Training				3		
Visitor Control				2		
Water Drainage				20		

Incident Degree of Seriousness

Form 7 lists the Degree of Seriousness (SE) for each incident (i.e., /threat/loss/asset combination). Refer to Section 5, Using RiskWatch A Step-By-Step Approach, for instructions on how to change the SE in RiskWatch. Use the SESA SE column to document any changes to the default SE.

Form 7 Degree of Seriousness

THREATS	LOSS CATEGORY	ASSET	R.W. SE	SESA SE
Air Conditioning Failure	Delays/Denials	Communications Hardware	4.0	
Air Conditioning Failure	Delays/Denials	Hardware	8.0	
Air Conditioning Failure	Delays/Denials	Personnel	8.0	
Air Conditioning Failure	Direct Loss	Support Systems	0.003	
Air Conditioning Failure	Related Direct Loss	Hardware	0.03	
Aircraft Accident	Delays/Denials	Communications Hardware	25.0	
Aircraft Accident	Delays/Denials	Facilities	150.0	
Aircraft Accident	Delays/Denials	Personnel	150.0	
Aircraft Accident	Delays/Denials	Support Systems	48.0	
Aircraft Accident	Delays/Denials	Utilities	24.0	
Aircraft Accident	Direct Loss	Communications Hardware	0.5	
Aircraft Accident	Direct Loss	Facilities	0.8	
Aircraft Accident	Direct Loss	Hardware	0.5	
Aircraft Accident	Direct Loss	Personnel	0.5	
Aircraft Accident	Direct Loss	Support Systems	0.5	
Biological Contamination	Delays/Denials	Personnel	25.0	
Biological Contamination	Direct Loss	Personnel	0.03	
Blackmail	Intangibles	Intangibles	0.3	
Bomb Threats	Delays/Denials	Personnel	2.0	
Budget Loss	Intangibles	Intangibles	0.5	
Chemical Spills	Delays/Denials	Personnel	48.0	
Cold/Frost/Snow	Delays/Denials	Facilities	50.0	
Cold/Frost/Snow	Delays/Denials	Personnel	16.0	
Cold/Frost/Snow	Delays/Denials	Support Systems	30.0	
Cold/Frost/Snow	Delays/Denials	Utilities	24.0	
Cold/Frost/Snow	Direct Loss	Facilities	0.01	
Cold/Frost/Snow	Direct Loss	Support Systems	0.15	
Cold/Frost/Snow	Intangibles	Intangibles	0.3	
Cold/Frost/Snow	Related Direct Loss	Facilities	0.15	
Cold/Frost/Snow	Related Direct Loss	Support Systems	0.15	
Communication Loss	Delays/Denials	Communications Hardware	15.0	
Communication Loss	Delays/Denials	Personnel	2.0	
Communication Loss	Direct Loss	Communications Hardware	0.35	
Communication Loss	Related Direct Loss	Communications Hardware	0.35	
Communication Loss	Related Direct Loss	Personnel	0.115	
Competition	Intangibles	Intangibles	0.5	
Currency Fluctuation	Intangibles	Accounts Payable	0.2	
Currency Fluctuation	Intangibles	Accounts Receivable	0.2	
Currency Fluctuation	Intangibles	Cash Accounts	0.2	
Data Destruction	Delays/Denials	Applications	15.0	

THREATS	LOSS CATEGORY	ASSET	R.W. SE	SESA SE
Data Destruction	Delays/Denials	Communications Software	15.0	
Data Destruction	Delays/Denials	Databases	100.0	
Data Destruction	Delays/Denials	System Software	30.0	
Data Destruction	Direct Loss	Databases	0.5	
Data Destruction	Modification	Databases	0.1	
Data Destruction	Related Direct Loss	Applications	0.015	
Data Destruction	Related Direct Loss	Communications Software	0.015	
Data Destruction	Related Direct Loss	Databases	0.015	
Data Destruction	Related Direct Loss	System Software	0.015	
Data Disclosure	Disclosure	Databases	0.09999	
Data Disclosure	Intangibles	Databases	0.01	
Data Disclosure	Intangibles	Intangibles	0.1	
Data Integrity Loss	Delays/Denials	Applications	50.0	
Data Integrity Loss	Delays/Denials	Communications Software	8.0	
Data Integrity Loss	Delays/Denials	Databases	35.0	
Data Integrity Loss	Delays/Denials	Procedures	8.0	
Data Integrity Loss	Delays/Denials	System Software	50.0	
Data Integrity Loss	Direct Loss	Accounts Payable	0.15	
Data Integrity Loss	Direct Loss	Accounts Receivable	0.15	
Data Integrity Loss	Direct Loss	Applications	0.15	
Data Integrity Loss	Direct Loss	Cash Accounts	0.06	
Data Integrity Loss	Direct Loss	Communications Software	0.15	
Data Integrity Loss	Direct Loss	Databases	0.1111	
Data Integrity Loss	Direct Loss	Procedures	0.15	
Data Integrity Loss	Direct Loss	Security	0.15	
Data Integrity Loss	Direct Loss	System Software	0.15	
Data Integrity Loss	Intangibles	Intangibles	0.0267	
Data Integrity Loss	Modification	Accounts Payable	0.001	
Data Integrity Loss	Modification	Accounts Receivable	0.001	
Data Integrity Loss	Modification	Applications	0.001	
Data Integrity Loss	Modification	Communications Software	0.001	
Data Integrity Loss	Modification	Databases	0.015	
Data Integrity Loss	Modification	System Software	0.001	
Data Integrity Loss	Related Direct Loss	Databases	0.15	
Earthquakes	Delays/Denials	Communications Hardware	16.0	
Earthquakes	Delays/Denials	Facilities	150.0	
Earthquakes	Delays/Denials	Hardware	150.0	
Earthquakes	Delays/Denials	Personnel	75.0	
Earthquakes	Delays/Denials	Support Systems	150.0	
Earthquakes	Delays/Denials	Utilities	50.0	
Earthquakes	Direct Loss	Communications Hardware	0.5	
Earthquakes	Direct Loss	Facilities	0.5	
Earthquakes	Direct Loss	Fire Detection/Sup	0.1	
Earthquakes	Direct Loss	Hardware	0.5	
Earthquakes	Direct Loss	Personnel	0.25	
Earthquakes	Direct Loss	Support Systems	0.5	
Earthquakes	Disclosure	Databases	0.25	
Earthquakes	Related Direct Loss	Personnel	0.25	
Electromagnetic Interference	Delays/Denials	Communications Hardware	10.0	

THREATS	LOSS CATEGORY	ASSET	R.W. SE	SESA SE
Electromagnetic Interference	Delays/Denials	Hardware	5.0	
Electromagnetic Interference	Direct Loss	Communications Hardware	0.5	
Electromagnetic Interference	Related Direct Loss	Communications Hardware	0.5	
Electromagnetic Interference	Related Direct Loss	Hardware	0.05	
Emanations	Delays/Denials	Databases	1.0	
Emanations	Direct Loss	Databases	0.25	
Emanations	Disclosure	Databases	0.1	
Errors, General/All	Delays/Denials	Accounts Payable	4.0	
Errors, General/All	Delays/Denials	Accounts Receivable	4.0	
Errors, General/All	Delays/Denials	Applications	5.0	
Errors, General/All	Delays/Denials	Communications Hardware	1.0	
Errors, General/All	Delays/Denials	Communications Software	2.0	
Errors, General/All	Delays/Denials	Databases	6.0	
Errors, General/All	Delays/Denials	Hardware	5.0	
Errors, General/All	Delays/Denials	Personnel	2.0	
Errors, General/All	Delays/Denials	System Software	2.0	
Errors, General/All	Direct Loss	Accounts Payable	0.10	
Errors, General/All	Direct Loss	Accounts Receivable	0.10	
Errors, General/All	Direct Loss	Cash Accounts	0.0005	
Errors, General/All	Direct Loss	Communications Hardware	0.0005	
Errors, General/All	Modification	Applications	0.3	
Errors, General/All	Related Direct Loss	Accounts Payable	0.005	
Errors, General/All	Related Direct Loss	Accounts Receivable	0.005	
Errors, General/All	Related Direct Loss	Applications	0.0005	
Errors, General/All	Related Direct Loss	Communications Hardware	0.005	
Errors, General/All	Related Direct Loss	Databases	0.005	
Errors, General/All	Related Direct Loss	Hardware	0.005	
Errors, General/All	Related Direct Loss	Personnel	0.005	
Fire, Catastrophic	Delays/Denials	Communications Hardware	150.0	
Fire, Catastrophic	Delays/Denials	Documentation	150.0	
Fire, Catastrophic	Delays/Denials	Facilities	150.0	
Fire, Catastrophic	Delays/Denials	Hardware	150.0	
Fire, Catastrophic	Delays/Denials	Personnel	75.0	
Fire, Catastrophic	Delays/Denials	Supplies and Consumable	24.0	
Fire, Catastrophic	Delays/Denials	Support Systems	48.0	
Fire, Catastrophic	Delays/Denials	Utilities	48.0	
Fire, Catastrophic	Direct Loss	Communications Hardware	0.3	
Fire, Catastrophic	Direct Loss	Documentation	0.5	
Fire, Catastrophic	Direct Loss	Facilities	0.5	
Fire, Catastrophic	Direct Loss	Hardware	0.8	
Fire, Catastrophic	Direct Loss	Office Equipment	0.1	
Fire, Catastrophic	Direct Loss	Personnel	0.05	
Fire, Catastrophic	Direct Loss	Supplies and Consumable	0.3	
Fire, Catastrophic	Direct Loss	Support Systems	0.9	
Fire, False Alarm	Delays/Denials	Personnel	2.0	
Fire, Major	Delays/Denials	Communications Hardware	25.0	
Fire, Major	Delays/Denials	Documentation	25.0	
Fire, Major	Delays/Denials	Facilities	25.0	
Fire, Major	Delays/Denials	Hardware	25.0	

THREATS	LOSS CATEGORY	ASSET	R.W. SE	SESA SE
Fire, Major	Delays/Denials	Personnel	25.0	
Fire, Major	Delays/Denials	Supplies and Consumable	12.0	
Fire, Major	Delays/Denials	Support Systems	25.0	
Fire, Major	Delays/Denials	Utilities	24.0	
Fire, Major	Direct Loss	Communications Hardware	0.2	
Fire, Major	Direct Loss	Documentation	0.21	
Fire, Major	Direct Loss	Facilities	0.25	
Fire, Major	Direct Loss	Hardware	0.2167	
Fire, Major	Direct Loss	Office Equipment	0.05	
Fire, Major	Direct Loss	Personnel	0.025	
Fire, Major	Direct Loss	Supplies and Consumable	0.15	
Fire, Major	Direct Loss	Support Systems	0.09	
Fire, Minor	Delays/Denials	Communications Hardware	8.0	
Fire, Minor	Delays/Denials	Documentation	8.0	
Fire, Minor	Delays/Denials	Facilities	8.0	
Fire, Minor	Delays/Denials	Hardware	8.0	
Fire, Minor	Delays/Denials	Personnel	8.0	
Fire, Minor	Delays/Denials	Supplies and Consumable	4.0	
Fire, Minor	Delays/Denials	Support Systems	8.0	
Fire, Minor	Delays/Denials	Utilities	8.0	
Fire, Minor	Direct Loss	Communications Hardware	.05	
Fire, Minor	Direct Loss	Documentation	.009	
Fire, Minor	Direct Loss	Facilities	.05	
Fire, Minor	Direct Loss	Hardware	.0433	
Fire, Minor	Direct Loss	Office Equipment	.01	
Fire, Minor	Direct Loss	Personnel	.005	
Fire, Minor	Direct Loss	Supplies and Consumable	0.03	
Fire, Minor	Direct Loss	Support Systems	0.015	
Flooding/Water Damage	Delays/Denials	Communications Hardware	48.0	
Flooding/Water Damage	Delays/Denials	Facilities	15.0	
Flooding/Water Damage	Delays/Denials	Hardware	24.0	
Flooding/Water Damage	Delays/Denials	Personnel	24.0	
Flooding/Water Damage	Delays/Denials	Supplies and Consumable	24.0	
Flooding/Water Damage	Delays/Denials	Utilities	24.0	
Flooding/Water Damage	Direct Loss	Communications Hardware	0.2	
Flooding/Water Damage	Direct Loss	Facilities	0.1	
Flooding/Water Damage	Direct Loss	Office Equipment	0.05	
Flooding/Water Damage	Direct Loss	Supplies and Consumable	0.05	
Flooding/Water Damage	Direct Loss	Support Systems	0.2	
Flooding/Water Damage	Related Direct Loss	Facilities	0.25	
Fraud/Embezzlement	Intangibles	Intangibles	0.5	
Fraud/Embezzlement	Modification	Accounts Payable	0.001	
Fraud/Embezzlement	Modification	Accounts Receivable	0.001	
Fraud/Embezzlement	Modification	Applications	0.001	
Fraud/Embezzlement	Modification	Cash Accounts	0.05	
Fraud/Embezzlement	Modification	Communications Software	0.001	
Fraud/Embezzlement	Modification	Negotiable Instruments	0.01	
Fraud/Embezzlement	Modification	System Software	0.001	
Hardware Failure	Delays/Denials	Personnel	4.0	

THREATS	LOSS CATEGORY	ASSET	R.W. SE	SESA SE
Hardware Failure	Related Direct Loss	Hardware	0.005	
Inflation	Direct Loss	Accounts Payable	0.25	
Inflation	Direct Loss	Accounts Receivable	0.25	
Inflation	Direct Loss	Cash Accounts	0.25	
Inflation	Intangibles	Accounts Payable	0.2	
Inflation	Intangibles	Accounts Receivable	0.2	
Inflation	Intangibles	Cash Accounts	0.2	
Misuse: Computer	Delays/Denials	Communications Software	15.0	
Misuse: Computer	Delays/Denials	Hardware	15.0	
Misuse: Computer	Delays/Denials	Personnel	4.0	
Misuse: Computer	Delays/Denials	Support Systems	30.0	
Misuse: Computer	Delays/Denials	System Software	50.0	
Nuclear Mishaps	Delays/Denials	Facilities	500.0	
Nuclear Mishaps	Delays/Denials	Personnel	500.0	
Power Loss	Delays/Denials	Communications Hardware	8.0	
Power Loss	Delays/Denials	Facilities	8.0	
Power Loss	Delays/Denials	Hardware	4.0	
Power Loss	Delays/Denials	Personnel	8.0	
Sabotage	Delays/Denials	Communications Hardware	16.0	
Sabotage	Delays/Denials	Facilities	15.0	
Sabotage	Delays/Denials	Hardware	16.0	
Sabotage	Delays/Denials	Personnel	10.0	
Sabotage	Delays/Denials	Utilities	8.0	
Sabotage	Direct Loss	Communications Hardware	0.5	
Sabotage	Direct Loss	Facilities	0.5	
Sabotage	Direct Loss	Hardware	0.5	
Sabotage	Related Direct Loss	Facilities	0.004	
Sabotage	Related Direct Loss	Personnel	0.0175	
Sinking Ground	Delays/Denials	Communications Hardware	16.0	
Sinking Ground	Delays/Denials	Facilities	150.0	
Sinking Ground	Delays/Denials	Hardware	24.0	
Sinking Ground	Delays/Denials	Personnel	8.0	
Sinking Ground	Direct Loss	Facilities	1.0	
Sinking Ground	Direct Loss	Support Systems	0.2	
Storms/Hurricanes	Delays/Denials	Communications Hardware	24.0	
Storms/Hurricanes	Delays/Denials	Facilities	20.0	
Storms/Hurricanes	Delays/Denials	Hardware	16.0	
Storms/Hurricanes	Delays/Denials	Personnel	8.0	
Storms/Hurricanes	Delays/Denials	Utilities	16.0	
Storms/Hurricanes	Direct Loss	Support Systems	0.2	
Storms/Hurricanes	Related Direct Loss	Facilities	0.25	
Substance Abuse	Delays/Denials	Personnel	20.0	
Substance Abuse	Related Direct Loss	Personnel	0.25	
Theft of Assets	Delays/Denials	Communications Hardware	24.00	
Theft of Assets	Delays/Denials	Hardware	25.00	
Theft of Assets	Delays/Denials	Office Equipment	15.00	
Theft of Assets	Delays/Denials	Supplies and Consumable	25.0	
Theft of Assets	Direct Loss	Communications Hardware	0.05	
Theft of Assets	Direct Loss	Hardware	0.05	

THREATS	LOSS CATEGORY	ASSET	R.W. SE	SESA SE
Theft of Assets	Direct Loss	Negotiable Instruments	0.05	
Theft of Assets	Direct Loss	Office Equipment	0.25	
Theft of Assets	Direct Loss	Supplies and Consumable	0.25	
Theft of Data	Delays/Denials	Databases	15.0	
Theft of Data	Direct Loss	Databases	0.90	
Theft of Data	Disclosure	Databases	0.10	
Theft of Data	Intangibles	Databases	0.05	
Theft of Data	Related Direct Loss	Databases	0.05	
Vandalism/Rioting	Delays/Denials	Facilities	25.0	
Vandalism/Rioting	Direct Loss	Facilities	0.0045	

Appendix B Sample Documents

Memo Announcing Review

FROM THE ANALYST TO EXECUTIVE MANAGEMENT

Date

TO: Mr. _________________, Director (Commissioner, etc)
Agency Name

FROM: Analyst
Risk Analysis Unit

SUBJECT: Risk Analysis Proposal

The Department of Labor (DOL) Unemployment Insurance Program Letter (UIPL) No. 34-87 requires all State Employment Security Agencies (SESA) to conduct risk analysis not less than once every three years. The SESAs use risk analysis to determine the effectiveness of internal controls. Attached is a draft proposal to conduct the required risk analysis for your review and approval.

I will contact your office to schedule a presentation during which I will provide an overview of risk analysis and request your approval of the proposal. If you have questions, contact me at (your phone number).

Memo from Executive to Unit(s) under Review

FROM THE CHIEF EXECUTIVE TO A DIVISION MANAGER

Date

TO: Mr/Ms---________ Division Manager
Name Unit To Be Review

FROM: ____________________, Director (Commissioner, etc.)
Agency's Name

SUBJECT: Risk Analysis of (the name of the business function under analysis)

Beginning (Date), the (Analyst Unit Name) will be conducting a Risk Analysis of the (name of business function or system). We will request the participation of several key employees in your division/unit, as well as the (Other Units associated with Unit under review). Their names are listed below to receive a copy of this memo. Please encourage them to fully cooperate with (Analyst Unit Name) to ensure this effort proves beneficial to the agency's operations.

Thank you for your cooperation in this matter.

cc: Name of Team Member
Name of Team Member
Name of Respondent
Name of Respondent
Name of Respondent

Memo to A Respondent

(Date)

To: Mr./Ms. ____________, Specialist
Information Systems Division

From: Analyst's Name
Analyst's Unit

Subject: Participation in Risk Analysis Respondent Program

The Internal Security Unit is currently conducting a risk analysis of, (business function named) including data processing systems necessary to (business function named). Due to your expertise in this area, you will be requested to participate as a respondent to a questionnaire program. Numerous other individuals from the (Other Areas) will also be asked to participate as respondents. Because the risk analysis will be conducted using automated risk analysis software, your responses must be made on a PC diskette which will be provided to you during the week of (Date). Completing this respondent program normally takes 30-60 minutes, and may be done at your own PC and at your own convenience.

The diskette provided to you will contain policy statements, procedural statements, statements concerning security precautions, etc. The program will ask you to assess levels of compliance or non-compliance to each policy, procedure, or security precaution on a scale of 0 to 100. How you score each statement should be based on your judgement, experience, opinion, etc.

All individual responses will be held as confidential; no individual response will be disclosed to any party. The responses you make will be loaded directly into a PC in the Internal Security Unit where the answers from all respondents will be automatically aggregated and analyzed along with much other data included in the software program.

An analysis, which is beneficial to the operations of the Department, as well as the employees of (business function named), will depend on your impartial consideration to the issues included in the respondent program. We appreciate your assistance. If you have questions please contact me (Telephone Number)

Memo to Respondent Requesting Return of Diskette

(Date)

TO: Respondent
Respondent's Unit

FROM: (Analyst Name), Specialist
(Analyst's Unit)

SUBJECT: Risk Analysis Questionnaire Diskette

Last (Date), you received a memo and questionnaire diskette as part of a risk analysis approved by the Director (Commissioner). The memo requested that you complete the questionnaire and return it to (name/unit) by (original due date). To date, I have not received your responses.

In the event that the original diskette become damaged or lost, I enclosed a duplicate diskette with instructions. Please complete the questionnaire and return it to me by (due date). If you are unable to complete the questionnaire by this date, or have questions, contact me at (your phone number).

Thank you for your assistance in this matter.

Proposal To Conduct Risk Analysis

DRAFT

PROPOSAL TO CONDUCT RISK ANALYSIS

System to be analyzed: The (Agency Name) (Business Function). This includes information systems used in (the business function).

Objectives of this risk analysis:

1). To identify vulnerabilities in (the business function under analysis) which could make the UI agency unable to accomplish its objectives or cause it to incur financial loss resulting from natural disasters, accidents, inefficiency, illegal acts, disgruntled employees, sabotage, terrorism, fraud, abuse, waste, and other causes.
2). To identify cost effective safeguards that will counteract the identified vulnerabilities and reduce risks to an acceptable level, as stated in OMB Circular No.-A-71.
3). To comply with DOL, OMB, and other regulations which require risk analysis.

Staffing: the (Analyst's Unit) staff will be responsible for conducting the large majority of the risk analysis workload.

Risk analysis team: A small group of experts from various sections/units will be necessary to compose a risk analysis team. Although it is not expected that team members will be required to invest extensive periods of time in the analysis, each team member should be available for brief consultations as needs arise.

The proposed team consists of:
(List Team Members)

Background/Methodology: The risk analysis will be conducted using an automated risk analysis software tool (RISKWATCH). This software was selected for SESA use by DOL as the result of the recent DOL sponsored National Risk Analysis Project. The software contains numerous interactive programs and databases developed to allow completion of risk analysis in a much shorter time period than required by manual risk analysis.

Questionnaire diskette process: The software also allows use of questionnaire diskettes distributed to various experts within the Department in order to assess levels of compliance to various security policies, procedures, precautions, etc. The use of questionnaire diskettes eliminates much of the interview and data gathering necessary with a manual risk analysis. The questions in the program were developed especially for SESA's use during the recent DOL National Risk Analysis Project.

Numerous experts within the Department will be requested to be respondents in the questionnaire program. While most of the questions on the diskette will relate specifically to each individual's area of expertise, some questions will apply to employees in general. Each expert may use his own personal computer in completing the questionnaire diskette. Completing the questionnaire normally takes 30-60 minutes, and may be done at a time that is convenient to the respondent. Questionnaires will be distributed to the experts. Other experts may be requested to participate as needed.

Asset analysis: Assets considered in this analysis will include UI funding, central office building facilities, UI applications, UI databases, and equipment in the Information Systems Operations Center which is necessary to (the business function under analysis).

Timeline: Should this proposal be accepted, Internal Security will make tentative plans to begin distribution of questionnaire diskettes to respondents on December 1. Using the automated software and the procedure as described above, we hope to complete the analysis in about months, circumstances permitting.

Reports: Prior to submitting the final Risk Analysis Report to the Director (Commissioner, etc.), a draft of the final report will be submitted to the Chief of UI, the Chief of Information Systems, and the (supervisor) of (the business function under analysis). This will allow interested parties to confer and potentially amend the draft version as appropriate. The DOL may request a copy of the final report.

STATEMENT OF UNDERSTANDING

The Statement of Understanding expresses agreements made between the State Employment Security Agencies (SESA) and the risk analysis team concerning the technical aspects of the work to be performed during the risk analysis.

PURPOSE:

RESTRICTIONS:

The risk analysis is not an audit.

SCOPE OF RISK ANALYSIS:

DIVISION (S) UNDER REVIEW:

RISK ANALYSIS SCHEDULE:

SIGNATURES:

______________________________ ______________________________

Center **Team Leader**

DATE: ______________________________

Appendix C RiskWatch Definitions

This appendix provides all the definitions used by RiskWatch. It includes definitions for Functional Areas, Loss Categories, Asset Categories, Threat Categories, Vulnerability Areas, and Safeguard Categories. The definitions appear as they do in RiskWatch. In some cases, the RiskWatch definition is incomplete; ellipse marks identify these definitions.

Functional Areas Listing

Category: Accounting
Unique ID: 1
Description: ACCOUNTING UNIT (ACC)- This area relates to the accounting unit of the organization. The unit that maintains the tax records and property tax information.

Category: Application Software Management
Unique ID: 2
Description: APPLICATION SOFTWARE MANAGEMENT (ASP) - This area relates to the computer applications programming and program support and maintenance function of the organization.

Category: Application/Program Security
Unique ID: 3
Description: APPLICATION PROGRAM SECURITY (APS) - This area relates to the specific application program security.

Category: Central/Program Office
Unique ID: 4
Description: CENTRAL OR PROGRAM OFFICE (CPO) - This area relates to the overall program management or central unit of an application program.

Category: Communications Management
Unique ID: 5
Description: COMMUNICATIONS MANAGEMENT (COM) - This area relates to the unit that operates and manages the communication systems and function of the organization.

Category: Computer Security Management
Unique ID: 6
Description: COMPUTER SECURITY OFFICER (CSO) - This area relates to the computer security function of the organization such as Computer Security Officer, Computer Security Manager, Computer Security Administrator, Computer Security Department etc.

Category: Computer Systems Operations
Unique ID: 7
Description: SYSTEMS OPERATIONS (SO) - This area relates to the computer operations function of the organization.

Category: Database Administration
Unique ID: 8
Description: DATABASE ADMINISTRATION (DBA) - This area relates to the unit that operates and manage the database systems of the organization.

Category: Designated Approving Authority
Unique ID: 9
Description: DESIGNATED APPROVING AUTHORITY (DAA) - This area relates to the managers that are responsible for the approval of the overall security and accreditation of the system or application.

Category: Document and Media Control
Unique ID: 10
Description: DOCUMENT & MAGNETIC MEDIA CONTROL (DMC) - This area relates to the unit that operates and manage the documentation library and the magnetic media (tape, disk and other media library) resources of the organization.

Category: Facilities Management
Unique ID: 11
Description: FACILITIES MANAGEMENT (CFM) - This area relates to the unit that operates and manage the facilities that supports the organization.

Category: Field Operations/End-User
Unique ID: 12
Description: FIELD OPERATIONS \ END-USER (USR) - This area relates to the end-users of the system or application.

Category: Financial Management/Budget
Unique ID: 13
Description: FINANCIAL MANAGEMENT & BUDGET (FMC) - This area relates to the financial and budget unit of the organization.

Category: Internal Audit and Investigations
Unique ID: 14
Description: INTERNAL AUDIT & INVESTIGATIONS (AUI) - This area relates to the internal audit and investigations unit of the organization.

Category: Mailroom
Unique ID: 15
Description: MAILROOM (MRS) - This area relates to the internal mailroom and supporting postal service unit of the organization.

Category: Network Management
Unique ID: 16
Description: NETWORK MANAGEMENT (NWM) - This area relates to the unit that operates and manages the local and wide area network systems and function of the organization.

Category: Office of Primary Responsibility
Unique ID: 17
Description: OFFICE OF PRIMARY RESPONSIBILITY (OPR) - This area relates to the owners of the databases and the managers that are responsible for the approval of the overall access permission and security of the specific databases.

Category: Personnel Services
Unique ID: 18
Description: PERSONNEL SERVICES (PSA) - This area relates to the unit that provides personnel and administrative services for the organization.

Category: Physical Security Officer
Unique ID: 19
Description: PHYSICAL SECURITY OFFICER (PSO) - This area relates to the physical security function of the organization such as Site Security Officer, Site Security Manager, Site Security Administrator, organization Security Department etc.

Category: Plans and Requirements
Unique ID: 20
Description: PLANS & REQUIREMENTS (PLN) - This area relates to the plans and long range requirements of the organization. It is a staff function related to resource allocation.

Category: Privacy Act Officer
Unique ID: 21
Description: PRIVACY ACT OFFICER (PAO) - This area relates to the specific function of the Privacy Act Officer as required by the Privacy Act of 1974. The Privacy Act mandates the appointment of a Privacy Act officer and specifies the minimum requirements for security.

Category: Program Policy Manager
Unique ID: 22
Description: PROGRAM POLICY MANAGER (PPM) - This area relates to the managers that are responsible for the policy and overall guidelines relative to the integrity and security of the system and application.

Category: Sensitive Materials Control
Unique ID: 23
Description: SENSITIVE MATERIALS CONTROL (SMC) - This area relates to the unit that is responsible for accountability and control of all sensitive material.

Category: Services Administration
Unique ID: 24
Description: SERVICES ADMINISTRATION (ADM) - This area relates to the unit that administers and manages the support services for the organization.

Category: Site Engineer and Maintenance
Unique ID: 25
Description: SITE ENGINEER & MAINTENANCE (SEM) - This area relates to the unit that provides engineering and maintenance support & services to the organization.

Category: Site Fire Marshal and Fire Department
Unique ID: 26
Description: SITE FIRE MARSHALL & FIRE DEPT. (SFM) - This area relates to the unit that provides fire safety inspections and fire fighting support.

Category: System Support Coordinator
Unique ID: 27
Description: SYSTEM SUPPORT COORDINATOR (SSC) - This area relates to the unit that provides support to the users of the system and application programs.

Category: Technical Support Manager
Unique ID: 28
Description: TECHNICAL SUPPORT MANAGER (SSM) - This area relates to the unit that provides operating system support to the operators, data base managers and application program units.

Category: Terminal Area Security
Unique ID: 29
Description: TERMINAL AREA SECURITY (TAS) - This area relates to the computer security function of the terminal areas or remote sites.

Category:	Warehouse
Unique ID:	30
Description:	WAREHOUSE (WHS) - This area relates to the unit that operates and manages the supplies, spare parts, forms and products supporting the organization.

Loss Categories Listing

Category: Delays/Denials
Unique ID: 1
Abbreviation: Interrupt
Description: Loss by Delays/Denials refers to losses of support, or loss of ability to provide services, or losses resulting from delays in support or in providing service, including depreciation of assets due to idle time.

Category: Direct Loss
Unique ID: 2
Abbreviation: Direct
Description: Direct Loss refers to losses such as theft of equipment or actual physical damage to assets.

Category: Disclosure
Unique ID: 3
Abbreviation: Disclosure
Description: Loss by Disclosure refers to the loss resulting from the disclosure of sensitive information.

Category: Intangibles
Unique ID: 4
Abbreviation: Intangible
Description: Intangible Loss refers to the loss of reputation, image, confidence, goodwill or credibility.

Category: Modification
Unique ID: 5
Abbreviation: Modification
Description: Loss by Modification refers to the loss by unauthorized changes to data.

Category: Related Direct Loss
Unique ID: 6
Abbreviation: Indirect
Description: Related Direct Loss refers to losses related to the primary loss, such as the halon, water or smoke removal after a fire, and administration of the recovery effort, etc.

Asset Categories Listing

Category Accounts Payable
Unique ID: 1
Abbreviation: Accts Pay
Description: ACCOUNTS PAYABLE - Includes all the money, including notes and loans, which the organization owes to any other entity.

Category Accounts Receivable
Unique ID: 2
Abbreviation: Accts Rec
Description: ACCOUNTS RECEIVABLE - Refers to all the money owed to the organization, including all outstanding invoices; all money billed, but not yet collected; and all long term loans.

Category Applications
Unique ID: 3
Abbreviation: Applicatns
Description: APPLICATIONS - Refers to special function programs usually developed for the system being analyzed such as inventory control, payroll, etc.

Category Cash Accounts
Unique ID: 4
Abbreviation: Cash Accts
Description: CASH ACCOUNTS - Refers to all the cash possessed by the organization, including petty cash.

Category Communications Hardware
Unique ID: 5
Abbreviation: Comms H/W
Description: COMMUNICATIONS/NETWORK HARDWARE - Communications assets include modems, multiplexers, cabling, communications boards, encryption devices, satellite dishes, antennas, and applicable software.

Category: Communications Software
Unique ID: 6
Abbreviation: Comms S/W
Description: COMMUNICATIONS/NETWORK SOFTWARE -

Category: Databases
Unique ID: 7
Abbreviation: Databases
Description: DATABASES - Refers to any data file used by any payroll, client eligibility programs, inventory listings, etc.

Category Documentation
Unique ID: 8
Abbreviation: Document'n
Description: DOCUMENTATION (TAPE AND DOCUMENTATION LIBRARIES) - Documentation refers to both manuals and hard copies of listings of programs and operating procedures used by the system.

Category: Facilities
Unique ID: 9
Abbreviation: Facilities
Description: FACILITIES - Facilities includes buildings as well as shared facilities such as coffee shops, employee lunches rooms, restrooms, etc.

Category: Fire Detection/Sup.
Unique ID: 10
Abbreviation: Fire Equip
Description: FIRE DETECTION AND SUPPRESSION SYSTEMS - Fire Detection and Suppression assets include smoke and alarms, fire alarms, humidity sensors, and fire suppression systems consisting of combinations of CO2, Water, or chemical foam.

Category: Hardware
Unique ID: 11
Abbreviation: Hardware
Description: HARDWARE - This category includes Central Processing Units (CPUs), printers, diskettes, tapes, controllers, mainframes, minis, micros, as well as "dumb" terminals.

Category: Intangibles
Unique ID: 12
Abbreviation: Intangible
Description: INTANGIBLES (REPUTATION) - This category includes considerations of a non-material nature such as the reputation of the organization and its credibility.

Category: Negotiable Instruments
Unique ID: 13
Abbreviation: Neg Instrs
Description: NEGOTIABLE INSTRUMENTS - Includes all stock certificates, bonds, food stamps, coupons, travelers cheques, gift certificates and any other item which could be exchanged for cash.

Category: Office Equipment
Unique ID: 14
Abbreviation: Off Equip
Description: OFFICE EQUIPMENT - Includes office desks, tables, chairs, filing cabinets, lamps, sofas, carpets, and any other type of office furniture.

Category: Personnel
Unique ID: 15
Abbreviation: Personnel
Description: PERSONNEL (AGENCY AND NAME) - Includes all support people of the organization including administrators, systems support people, operators, users, and any person who has anything to do with the system.

Category: Procedures
Unique ID: 16
Abbreviation: Procedures
Description: PROCEDURES (AGENCY) - This category includes the operating procedures of the system, including procedures for hiring, administrative procedures, and procedures for emergency response.

Category: Security
Unique ID: 17
Abbreviation: Security
Description: SECURITY SYSTEMS (AGENCY) - Includes motion detectors, video cameras, access control systems, card key systems, locks, safes, security software (such as TOP SECRET), password programs, fences, and encryption devices.

Category: Supplies and Consumable
Unique ID: 18
Abbreviation: Supplies
Description: SUPPLIES AND CONSUMABLES (NAME AND AGENCY WAREHOUSES) - Includes office supplies such as paper, ribbons, tapes, disks, folders, pens, pencils, etc.

Category: Support Systems
Unique ID: 19
Abbreviation: Suppt Sys
Description: SUPPORT SYSTEMS - Includes air conditioning systems, heating systems, humidifying systems, fuel systems, cooling systems for machinery and grounding systems.

Category: System Software
Unique ID: 20
Abbreviation: System S/W
Description: SYSTEM SOFTWARE - Includes job language programs and all operating system programs, such as DOS, CPM, UNIX, OS, GCOS, VMS, etc.

Category: Utilities
Unique ID: 21
Abbreviation: Utilities
Description: UTILITIES (ELECTRICAL POWER) - Includes electrical power, telephone systems, natural gas, water and fuel.

Threats Listing

Category: Air Conditioning Failure
Unique ID: 1
Abbreviation: AirCo Fail
Description: AIR CONDITIONING FAILURE - Air Conditioning Failure. This threat is a major cause of computer malfunctions. Both hardware and software should be kept at 70-90 degrees F. to assure proper functioning. High temperatures may cause semi-conductors to break down and produce flawed data. Local Data is usually available on failures per year.

Category: Aircraft Accident
Unique ID: 2
Abbreviation: Air Accidt
Description: AIRCRAFT ACCIDENT - The threat of aircraft accident has increased over the last thirty years. Frequency of occurrence is increased over 100 times if the facility is located near the flight path. Frequency also increased if the facility is located near the take-off or landing pattern of an airport or military base.

Category: Biological Contamination
Unique ID: 3
Abbreviation: Biol Contm
Description: BIOLOGICAL CONTAMINATION - Biological contamination refers to the threat of contagious disease in a work environment. Unsanitary conditions in a common lunchroom may spread flu or cold viruses. Re-circulating air conditioning systems can cause respiratory problems including Legionnaire's Disease.

Category: Blackmail
Unique ID: 4
Abbreviation: Blackmail
Description: BLACKMAIL - Blackmail is a threat to an individual who is in a position to get sensitive information from the computer, to modify or destroy data. If the computer center handles financial, sensitive, or privacy information, this threat increases.

Category: Bomb Threats
Unique ID: 5
Abbreviation: Bomb Thrt
Description: BOMB THREATS - Because Bomb Threats are potentially very destructive, they must be taken seriously, and so can be used by insiders to create an opportunity for theft, or data modification. A related loss is personnel time and work lost.

Category: Budget Loss
Unique ID: 6
Abbreviation: Budgt Loss
Description: BUDGET LOSS - Budget loss can threaten any department or agency that must submit budgets and get approval for continued funding. Budget cuts in the ADP center may result in loss of prime resources, from personnel to technical equipment.

Category: Chemical Spills
Unique ID: 7
Abbreviation: Chem Spill
Description: CHEMICAL SPILLS - Chemical spills may immobilize computer center personnel, cause widespread illness, or prevent employees from reaching their jobs. This threat is more likely to occur when the computer center is located in a highly industrial area.

Category: Cold/Frost/Snow
Unique ID: 8
Abbreviation: Frost/Snow
Description: COLD/FROST/SNOW - Cold/Frost/Snow are a major threat in many areas of the U.S. Cooling systems can freeze, pipes can rupture, crack and burst. At risk are water pipes, fuel pipes, and lubricating systems.

Category: Communication Loss
Unique ID: 9
Abbreviation: Comms Loss
Description: COMMUNICATION LOSS - Communications failure covers breakdown in the communication system including the operator, phone lines, communication concentrator, wires, hardware and software related to this system. NOTE: Does not include internal communication.

Category: Competition
Unique ID: 10
Abbreviation: Competitn
Description: COMPETITION - Competition relates to data stolen or disclosed to competitors resulting in harm to the organization. Also refers to loss of key personnel to the competition, where they gain an experienced employee as well as inside information.

Category: Currency Fluctuation
Unique ID: 11
Abbreviation: Curr Fluct
Description: CURRENCY FLUCTUATION - Currency fluctuation primarily affects organizations dealing in the international marketplace who pay for services (such as telephone lines), or personnel, with foreign currency. For example, the peso recently dropped 500% in one day.

Category: Data Destruction
Unique ID: 12
Abbreviation: Data Destr
Description: DATA DESTRUCTION - Data Destruction covers all the ways that computer data can be destroyed, including inadvertent error, program "bugs", overt acts, covert acts (by insiders), and computer viruses.

Category: Data Disclosure
Unique ID: 13
Abbreviation: Data Discl
Description: DATA DISCLOSURE - Data Disclosure always results in a loss to the legitimate data owner, and gain to the competitor (incl. foreign govt.'s.). Disclosure can cause the death of a special agent, bad publicity for the responsible agency, or the loss of secrets

Category: Data Integrity Loss
Unique ID: 14
Abbreviation: Integ Los
Description: DATA INTEGRITY LOSS - The loss of Data Integrity deals with corruption of computer data, reducing confidence in the accuracy of the data by the end user. Also refers to insider tampering to increase pay, or adding money to personal accounts.

Category: Earthquakes
Unique ID: 15
Abbreviation: E'quakes
Description: EARTHQUAKES - The threat of earthquake combines several other threats including the explosions resulting from gas leaks after the quake, major and minor fires, loss through injury and loss of life.

Category: Electromagnetic Interference
Unique ID: 16
Abbreviation: E/M Interf
Description: ELECTROMAGNETIC INTERFERENCE - Electromagnetic propagation relate to any form of radiation (including cosmic radiation such as sunbursts) that affect communication circuits and computer components, causing changes in data characteristics.

Category: Emanations
Unique ID: 17
Abbreviation: Emanations
Description: EMANATIONS - Emanations are intelligent signals inadvertently broadcast by a communication system, computer, or other electronic device. Also known as "compromising emanations", they can disclose sensitive information at a low signal strength.

Category: Errors, General/All
Unique ID: 18
Abbreviation: Errors
Description: ERRORS GENERAL/ALL - Error and reduced efficiency are, by definition, unintentional, but they can result in compromising information, loss of data integrity, and data destruction. Errors can be caused by people, faulty programs/equipment or by design flaw.

Category: Fire, Catastrophic
Unique ID: 19
Abbreviation: Fire Catas
Description: FIRE, CATASTROPHIC - Catastrophic fire refers to a fire involving very large losses. In a catastrophic fire, most of what was threatened is actually lost.

Category: Fire, False Alarm
Unique ID: 20
Abbreviation: Fire False
Description: FIRE, FALSE ALARM - False alarms effect loss of time in the workplace and loss of efficiency, as well as delays and denials of service to the end users. Most false alarms are caused by fire system detection malfunctions.

Category: Fire, Major
Unique ID: 21
Abbreviation: Fire Major
Description: FIRE, MAJOR - Major fires result in approximately 10% of what is threatened actually being lost. In orders of magnitude, a minor fire occurs 10 times more often than a major fire and a major fire 10 times more often than a catastrophic fire.

Category: Fire, Minor
Unique Id: 22
Abbreviation: Fire Minor
Description: FIRE, MINOR - Minor fires occur ten times more often than major fires. In a minor fire, less than one percent of what is threatened is lost.

Category: Flooding/Water Damage
Unique ID: 23
Abbreviation: Flooding
Description: FLOODING/WATER DAMAGE - Flooding and water damage result in destruction due to flooding from storms, broken pipes, or broken dams. Water damage resulting from fire is grouped under the threat of "fire".

Category: Fraud/Embezzlement
Unique ID: 24
Abbreviation: Fraud/Embz
Description: FRAUD/EMBEZZLEMENT - Fraud and embezzlement is the most common computer crime, but the most difficult to detect. This threat materializes through the manipulation of programs, databases, hardware systems, communication systems, administrative and personnel.

Category: Hardware Failure
Unique ID: 25
Abbreviation: H/W Fail
Description: HARDWARE FAILURE - Hardware and systems failure refer to any failure in the computer hardware, the central processing unit (CPU), memory, and peripherals. These types of failures can result in long delays because the entire system must be restarted after correction.

Category: Inflation
Unique ID: 26
Abbreviation: Inflation
Description: INFLATION - Inflation is considered a threat when the price of services, products, consumables and operational costs increase and the increases are not reflected in budgetary increases, resulting in reduced services and support.

Category: Misuse: Computer
Unique ID: 27
Abbreviation: Misuse/Com
Description: MISUSE COMPUTER - Misuse of computer time is prevalent in most computer centers and is related to personnel using computer resources for their own personal benefit. This type of abuse results in higher usage figures than are real and affect planning.

Category: Nuclear Mishaps
Unique ID: 28
Abbreviation: Nuclear
Description: NUCLEAR MISHAPS - When a facility is located within thirty miles of a nuclear plant, there is increased likelihood of losses resulting from nuclear explosion/contamination which could cause a quarantine in the area until the radiation level becomes safe.

Category: Pirating Key Personnel
Unique ID: 29
Abbreviation: Pirating
Description: PIRATING KEY PERSONNEL - This threat cover the loss of key employees who represent an investment to the agency in terms of training and staffing. Major losses can result from the loss of proprietary and sensitive information including strategic plans, financial data, internal problems, etc.

Category: Power Loss
Unique ID: 30
Abbreviation: Power Loss
Description: POWER LOSS - Refers to losses attributed to the loss of electrical power from the primary sources, including transformer failures, breaker failures, phase unbalance and circuit overloading.

Category: Resource Mismanagement
Unique ID: 31
Abbreviation: Res Mismgt
Description: RESOURCE MISMANAGEMENT - Resource mismanagement refers to poor management practices such as lack of coordination, lack of synergy, lack of planning, and poor use of available resources, including personnel.

Category: Sabotage
Unique ID: 32
Abbreviation: Sabotage
Description: SABOTAGE - Sabotage and terrorism apply to the placement of explosive devices, destruction by overt or covert means of tangible resources, such as electrical, air conditioning systems, hardware and facilities; as well as intangibles such as information.

Category: Sinking Ground
Unique ID: 33
Abbreviation: Sink Grnd
Description: SINKING GROUND - Subsidence and ground sinking apply only to areas with unstable ground and where much ground shifting (subsidence) can be expected. This is especially important when selecting a new site for a facility.

Category: Storms/Hurricanes
Unique ID: 34
Abbreviation: Storms
Description: STORMS/HURRICANES - Storms, hurricanes, tornadoes, typhoons, and tsunamis include high velocity winds accompanied by rain, which cause a great deal of damage to anything in their path. Frequency of occurrence estimates varies greatly depending on geography.

Category: Substance Abuse
Unique ID: 35
Abbreviation: Subs Abuse
Description: SUBSTANCE ABUSE - Refers to use of alcohol and controlled substances by personnel. Excessive absenteeism, lack of concentration, high turnover, increased accident and error rates; and poor quality work are all related to alcohol and drug abuse.

Category: Theft of Assets
Unique ID: 36
Abbreviation: Theft Asst
Description: THEFT OF ASSETS - Theft of assets covers the actual loss of resources from both insiders and outsiders. Frequency of occurrence is best obtained from inventory control maintenance records. NOTE: Losses are almost always higher than documented.

Category: Theft of Data
Unique ID: 37
Abbreviation: Theft Data
Description: THEFT OF DATA - Theft of data is extremely difficult to detect. Data can be stolen without being missed. It can be stolen with no physical contact, through communication lines, or by monitoring emanations. Data losses can be extremely damaging.

Category: Vandalism/Rioting

Unique ID: 38

Abbreviation: Vandl/Riot

Description: VANDALISM/RIOTING - This threat refers to civil disorder and materializes when company personnel or outsiders behave as a mob, looting, destroying property, disrupting operations and threatening personal safety.

Vulnerability Areas Listing

Category: Access Control
Unique ID: 1
Description: ACCESS CONTROL - Access control covers weaknesses related to allowing unauthorized entry into the application under review. Includes weaknesses in physical access, such as lack of visitor's logs, lack of physical locks, inadequate or non-existent password.

Category: Accountability
Unique ID: 2
Description: ACCOUNTABILITY - Accountability refers to weaknesses in the assigning of areas of responsibility for various components of the system or application under review, responsibility for physical assets, for procedures, or for implementing policy.

Category: Administration
Unique ID: 3
Description: ADMINISTRATION - Administration refers to weaknesses related to the management component of the organization, the people who run the organization, specifically, those who organize, staff and administer the system under review.

Category: Application
Unique ID: 4
Description: APPLICATION - Application refers to weaknesses which relate to the program or system under review and to the tasks that are program related, i.e. payroll, inventory control, sorting, check writing and validation programs.

Category: Audit Trails
Unique ID: 5
Description: AUDIT TRAIL - Audit trail weaknesses refer to the lines of procedure and accountability in the organization; specifically, lack of a traceable record of every transaction created by the system. Weaknesses in this area affect the capability of the system

Category: Compliance
Unique ID: 6
Description: COMPLIANCE - Compliance weaknesses relate to lack of compliance with organizational procedures and requirements. For example, if the organization requires that a risk analysis be performed every three years, then the act of not performing the risk analysis

Category: Construction
Unique ID: 7
Description: CONSTRUCTION - Construction weaknesses lie in the area of physical facilities, such as hinges on the outside of doors, rooms with half walls, etc.

Category: Contingency Plan
Unique ID: 8
Description: CONTINGENCY PLAN - Refers to the lack of a workable contingency plan, or lack of implementation of a contingency plan where one exists already. This is considered a major weakness in any organization.

Category: Data Integrity
Unique ID: 9
Description: DATA INTEGRITY - Data integrity weaknesses refer to lack of program controls, lack of access control for databases, lack of validation, lack of audit trails related to data, lack of passwords related to data, or any weakness that would adversely affect the data integrity.

Category: Disclosure
Unique ID: 10
Description: DISCLOSURE - Disclosure weaknesses relate to anything that might contribute to the unintentional disclosure of data, such as lack of access controls, lack of encryption devices, lack of control of compromising emanations, lack of accountability of sensitive…

Category: Documentation
Unique ID: 11
Description: DOCUMENTATION - Documentation weaknesses refer to insufficient, unavailable or incorrect documentation.

Category: Emergency Response
Unique ID: 12
Description: EMERGENCY RESPONSE - Weaknesses related to emergency response include all the elements of the organization's response to an emergency situation, such as assigning of duties, having personnel resources identified, having adequate resources such as tools,…..

Category: Evaluation
Unique ID: 13
Description: EVALUATION - Weaknesses in the area of evaluation, or determination of status, refer to the lack of analysis, lack of surveys, lack of systems testing, etc.

Category: Fire
Unique ID: 14
Description: Fire - Weaknesses in the area of fire include lack of functional fire suppression and detection systems, lack of emergency response (how to respond in case of an actual fire), lack of training in the procedures to be followed in the event of fire, etc.

Category: Labeling
Unique ID: 15
Description: LABELING - Labeling weaknesses refer to lack of appropriate labeling in relation to sensitivity levels and distribution; incorrect labeling, incorrect routing by labels, etc.

Category: Maintenance
Unique ID: 16
Description: MAINTENANCE - Maintenance weaknesses refer to inadequate, incorrect, or insufficient maintenance; lack of preventive maintenance, etc.

Category: Organization
Unique ID: 17
Description: ORGANIZATION - Organizational weaknesses refer to lack of organizational structure, including lack of specific assignments and assigned accountability, incorrect reporting structure, lack of functional separation of duties, lack of definitive policy, etc

Category: Policy
Unique ID: 18
Description: POLICY - Weaknesses in the area of policy refer to incorrect policies, insufficient policies, lack of implementation of existing policies, etc.

Category: Privacy Act
Unique ID: 19
Description: PRIVACY ACT - Weaknesses in the area of Privacy Act refer to not identifying Privacy Act records and files, not reporting Privacy files to the Federal Register, not allowing distribution of Privacy Act guidelines, insufficient Privacy Act training, and i…

Category: Procedures
Unique ID: 20
Description: PROCEDURES - Weaknesses in the area of procedures refer to lack of proper procedures, insufficient procedures, unimplemented procedures or incorrect procedures.

Category: Reliability
Unique ID: 21
Description: RELIABILITY - Weaknesses in the area of reliability refer to lack of accuracy, lack of reliability, lack of system validation, lack of availability, lack of confidence in the data, etc.

Category: Tempest
Unique ID: 22
Description: TEMPEST - Weaknesses in the area of Tempest apply to Department of Defense systems only. They include lack of shielding, lack of filtering, lack of grounding and lack of proper evaluation of compromising emanations.

Category: Terminal Site
Unique ID: 23
Description: TERMINAL SITE - Weaknesses in the terminal site refer to lack of access controls, lack of emergency response, lack of audit trails, lack of policy and procedures, as they relate to the terminal area.

Category: Training
Unique ID: 24
Description: TRAINING - Weaknesses in the area of training include lack of adequate funding, lack of technical support for training, lack of policies regarding training, lack of training time and materials and lack of emphasis on training.

Safeguards Listing

Category: Physical Access Control
Unique ID: 1
Description: PHYSICAL ACCESS CONTROL - The Access Control safeguard refers to the existence of a verifiable and coordinated access control system. The system can range from simple (key lock systems) to complex (cipher/key card identification systems).

Category: Application Controls
Unique ID: 2
Description: APPLICATION CONTROL STANDARDS - Application control refers to a specific system of controls designed by a team of internal auditors to ensure that universal programming standards, data element dictionaries and record association conventions are maintained.

Category: Audit Trails
Unique ID: 3
Description: AUDIT TRAILS - The safeguard of Audit Trails refers to the organization having a fully implemented audit trail capability so that it is simple to track which user was accessing any system at any point in time.

Category: Classification Markings
Unique ID: 4
Description: CLASSIFICATION MARKING - The safeguard of Classification Marking refers to having all media and reports containing information which is classified as Classified, Sensitive, or Privacy Act data marked on the top and bottom of each page.

Category: Contingency Plan
Unique ID: 5
Description: CONTINGENCY PLAN - The Contingency Plan is also known as a Continuity of Operations Plans (COOP), or as a Disaster Recovery Plan. It contains a detailed blueprint of backup procedures to be followed in case of emergency disruption to the ADP facility, as well as a guide to getting the programs operational as quickly as possible.

Category: Contract Specifications
Unique ID: 6
Description: CONTRACT SPECIFICATIONS - The Contract Specification safeguard refers to the practice of requiring each contractor to include as a formal contract deliverable, a plan for including appropriate security controls and addressing of pertinent threats.

Category: Data Encryption
Unique ID: 7
Description: DATA ENCRYPTION - This safeguard involves the application of encipherment techniques to one or more data sets or to data travelling over communications systems.

Category: Detection System
Unique ID: 8
Description: DETECTION SYSTEM - The Detection System safeguard refers to having a coordinated fire detection/access control violation system which will alert the proper authorities to smoke, heat, water, humidity fluctuations, grounding problems, as well as monitoring any attempt at unauthorized access.

Category: Documentation
Unique ID: 9
Description: DOCUMENTATION - The Documentation safeguard refers to the need for the organization to provide backup documentation for every file, program, and process; including providing hard copies retained in a safe location.

Category: Electrical Power
Unique ID: 10
Description: ELECTRICAL POWER CONDITIONING - The Electrical Power Conditioning safeguard refers to the establishment of a stable sources of electrical power, including a consideration of a source of uninterruptible power, backup generators, as well as consideration of phase-balancing to prevent power fluctuations.

Category: Emergency Response
Unique ID: 11
Description: EMERGENCY RESPONSE - The emergency response safeguard deals with a having a detailed guide of how the organization can continue to operate in the event of large scale emergencies, such as chemical spills, civil disobedience, or nuclear mishaps.

Category: File/Pgm. Control (DAC)
Unique ID: 12
Description: FILE/PROGRAM CONTROL - The safeguard of File/Program Control refers to the practice of establishing a system of access controls and authorizations for programs and files based on "need to know".

Category: Fire Suppression
Unique ID: 13
Description: FIRE SUPPRESSION SYSTEM - The Fire Suppression safeguard refers to the appropriate combination of water and CO2, which should be installed in any ADP facility.

Category: Grounding System
Unique ID: 14
Description: GROUNDING SYSTEM - The Grounding System safeguard refers to provision for proper electrical grounding for all equipment, including lightning arrestors; a separate grounding system for all signal cables. For sites processing classified information, a local low resistance ground is required.

Category: Insurance/Bond
Unique ID: 15
Description: INSURANCE - Insurance policies should be considered as a safeguard for situations where other types of safeguards might not be currently available or cost-effective. Financial institutions should consider bonding insurance for key personnel.

Category: Life Cycle Management
Unique ID: 16
Description: LIFE CYCLE MANAGEMENT - The safeguard of Life Cycle Management refers to the adoption of a formal, written plan for all systems, including security and audit controls. This plan should address general management, personnel, organizational, system design, data center management, and computer applications controls.

Category: Material Segregation
Unique ID: 17
Description: MATERIAL SEGREGATION - The Material Segregation safeguard refers to the procedure of separating Classified, Sensitive and Privacy Act data from all other material in order to guard against inadvertent disclosure.

Category: Monitor System
Unique ID: 18
Description: MONITOR SYSTEM - The Monitoring System safeguard refers to having an effective system in place which covers checking of remote sites, critical components, operational status of various programs and applications as well as sensitive operational areas.

Category New Construction
Unique ID: 19
Description: NEW CONSTRUCTION - The New Construction safeguard covers a variety of considerations, which should be reviewed for any new facility. These include, but are not limited to, use of fire retardant and low combustion building materials, use of floor-to-ceiling walls, automatic vent closure, inside hinges on doors and windows, and proper drainage.

Category: Operating Procedures
Unique ID: 20
Description: OPERATING PROCEDURES - The safeguard of operating procedures refers to having a monitoring program in place in order to determine the effectiveness and efficiency of the system's operating procedures, as well as a method of monitoring that these procedures are continuously upgraded.

Category: OPR for each System
Unique ID: 21
Description: OFFICE OF PRIMARY RESPONSIBILITY (OPR) - An Office of Primary Responsibility (OPR) should be designated for each database, data file, and removable media containing data or programs. The OFFICE OF PRIMARY RESPONSIBILITY designation is necessary to ensure integrity of data files and accuracy of their contents.

Category: Organizational Structure
Unique ID: 22
Description: ORGANIZATIONAL STRUCTURE - Organizational structure refers to the safeguard of having the organization not only staffed, but also responsive to the need for redundancy of critical job functions and that the necessary guidelines are in place to ensure functional separation of duties.

Category: Passwords/Authentication
Unique ID: 23
Description: PASSWORDS - The safeguard of Passwords refers to the organization having an effective policy of user passwords that should be fully implemented for every system.

Category: Personnel Clearances
Unique ID: 24
Description: PERSONNEL CLEARANCE - The Personnel Clearance safeguard refers to having an organizational policy governing personnel clearance in which each individual must have a security clearance of equal or greater classification than the highest level of data processed in the system they are accessing. This safeguard also includes background investigation of all employees.

Category: Personnel Control
Unique ID: 25
Description: PERSONNEL CONTROL - The safeguard of Personnel Control refers to the organization having proper procedures for automatic background checks, authority based on "need to know" criteria, as well as timely method for updating personnel records when individual are reassigned, transferred or discharged.

Category: Preventive Maintenance
Unique ID: 26
Description: PREVENTIVE MAINTENANCE - The Preventive Maintenance safeguard refers to having an effective maintenance program in place which should include all computer hardware, generators, air conditioning equipment, grounding systems, lightning arrestors, fire system and structured components such as vent closures, floor plates, doors, etc.

Category: Property Management
Unique ID: 27
Description: PROPERTY MANAGEMENT - The Property Management safeguard refers to the organization having a comprehensive and effective program for property inventory control, allocation and accountability.

Category: Quality Assurance
Unique ID: 28
Description: QUALITY ASSURANCE - The safeguard of Quality Assurance refers to the formal establishment of a program, which will regularly, monitor (and find ways to improve) programming quality, user error, communication ability, etc.

Category: Redundant Power
Unique ID: 29
Description: REDUNDANT POWER - The safeguard of Redundant Power refers to having a secondary independent source of electrical power to backup the primary power source.

Category: Review Sens. Applications
Unique ID: 30
Description: REVIEW OF SENSITIVE APPLICATIONS - The safeguard of Review of Sensitive Applications refers to the need of the organization to conduct a formal risk assessment of each Sensitive Application program on a regular basis.

Category Risk Analysis
Unique ID: 31
Description: RISK ANALYSIS - The safeguard of Risk Analysis refers to the organization having recently conducted a formal risk assessment of each major system and application program.

Category: Security Classification
Unique ID: 32
Description: SECURITY CLASSIFICATION - The Security Classification safeguard requires that each activity have policies in place addressing the proper classification of sensitive materials, including a receipt program, and general handling procedures for all sensitive and classified materials.

Category: Security Plan
Unique ID: 33
Description: SECURITY PLAN - The Security Plan refers to the existence of a document which defines the tasks and charges of the security organization; as well as planning the security procedures necessary for the protection of the organization.

Category: Security Policy
Unique ID: 34
Description: SECURITY POLICY - Security policy refers to the existence of written, defined guidelines which dictate how the organization manages its resources and protects them from both internal and external threats.

Category: Security Staff
Unique ID: 35
Description: SECURITY STAFF - The Security Staff refers to the individuals in the organization who maintain or manage security tasks, as well as addressing full-time security staff, include managers who have part-time security responsibilities for the resources they manage.

Category: Safeguard Test & Eval.
Unique ID: 36
Description: SYSTEM SECURITY TEST AND EVALUATION (SST&E) - The safeguard of SST&E (System Security Test and Evaluation) refers to the organization having a formal procedure to test each individual safeguard for effectiveness and accuracy.

Category: System Validation
Unique ID: 37
Description: SYSTEM VALIDATION - The System Validation safeguard refers to the practice of ensuring that the operating system contains only approved code; and that changes to the operating system are accounted for, are verified, and are transmitted in a secure and acknowledged mode.

Category: Technical Surveillance
Unique ID: 38
Description: TECHNICAL SURVEILLANCE - This safeguard is applicable to classified environments and refers to a (possibly external) organization that can conduct a survey to identify potential security problems.

Category: Tempest Survey
Unique ID: 39
Description: TEMPEST SURVEY - This safeguard is applicable to Classified environments and refers to the gathering of information, by inspection or survey, about all instrumentation and sites that store or process classified information.

Category: Training
Unique ID: 40
Description: TRAINING - The training safeguard refers to the organization having a written implemented program for security training of new employees, and security awareness programs for current employees.

Category: Visitor Control
Unique ID: 41
Description: VISITOR CONTROL - The visitor control safeguard refers to ensuring that visitors to a facility are monitored twenty-four hours a day, that an audit trail of visitors exists and that this official record is maintained for at least two years.

Category: Water Drainage
Unique ID: 42
Description: WATER DRAINAGE - The Water Drainage safeguard refers to ensuring that the facility is equipped with a drainage system so that water from broken pipes, water from activated sprinkler systems or water used in fire fighting can be easily and effectively drained from the facility.

Index