MINICOMPUTER SYSTEMS
COST-RISK ANALYSIS AND IMPACT ANALYSIS

1.   GENERAL

1.01 This section addresses economic
     criteria dealing with risks, costs, and
impact of providing or not providing
security and recovery capabilities.

1.02 Whenever this section is reissued, the
     reason(s) for reissue will be given in
this paragraph.

1.03 Decisions to commit corporate
     resources to security and recovery
capabilities must be based on a realistic
evaluation of the impact on the company
should data integrity be compromised or
should the minicomputer facility be

destroyed or severely impaired.

1.04 Company information stored on
     minicomputer systems is a very valuable
company asset. This information (data)
must be protected from loss, destruction,
or external access. This protection can be
achieved
by installing data security protective
measures. Implementation of such measures
needs to be based upon the cost of potential
loss, the risk of loss, and the cost of the
protective measure itself. A process usable
in determining the feasibility of imple-
menting protective measures is called
cost-risk analysis.

1.05 "Cost-risk" and "cost-benefit"
     analysis are methods that can be used
to determine if a protective measure is
cost justifiable. The emphasis of such
analysis is to make an intelligent compro-
mise between providing adequate security
and committing funds to such implementation.

2.   DATA SECURITY FACTORS

2.01 Cost-risk analysis for data requires
     the estimation of the potential dollar
value loss for each element of data
requiring protection. The indirect costs
of loss such as idle resources or loss of
sales opportunity must be considered, as
well as direct costs such as theft of money
or equipment. The incurred cost should be
viewed on a per loss basis. The following
items should be considered when making this
estimation:

   (a) Cost to reconstruct lost or damaged
       data.

(b) Costs due to delayed or missed processing, such as idle resources and missed commitments.

(c) Costs due to the loss of assets such as fraudulent equipment orders or misappropriation of funds.

(d) Costs due to the loss or disclosure of revenue producing data.

(e) Costs affecting customer service resulting from inaccurate data.

(f) Costs due to loss or disclosure of data which weakens the company's competitive position.

(g) Cost of possible legal penalties if improper information is dislosed.

2.02 After the cost of a loss has been determined, it is necessary to estimate the probability frequency of such loss. Occurrence frequency needs to be annualized in order to conform to annual cost criteria (i.e. - the probable frequency of a loss should be stated as number per year). For example, if probable frequency is twice a month, the annualized probability of frequency equals 24. If the frequency is once every two months, then the annualized probability of frequency equals 6.

2.03 The expected per element yearly loss is calculated by multiplying the annual probable frequency of loss occurrences by the potential loss per occurrence estimate. The amounts for each calculated element are then summed to estimate the total expected yearly loss. This number is now used as a guide for determining the amount of money which is reasonable to spend on protective measures.

2.04 The costs of protective measures fall into two major divisions: initial costs and ongoing costs. Initial costs include the purchase or lease of new system elements, modification of existing systems to accept the new protective measure, one-time administrative actions to support the new measures, and the initial testing of their effectiveness. Ongoing costs reflect the increased day-to-day costs of running the system with the protection enhancements which should include such items as personnel, minicomputer processing, storage, and system monitoring.

2.05 A low cost protective measure may and most likely should be selected without reference to extensive cost-risk analysis. Some form of cost-risk analysis or other economic justification must be performed for moderate cost protective measures. A detailed cost-risk analysis should be performed for high cost protective measures (see subsection 4 for possible exception). A detailed analysis includes:

(a) One time implementation costs, amortized over the expected system life span to develop an annual effect of implementation cost.

(b) Annual ongoing costs.

2.06 High cost protective measures are selected based on the following criteria:

(a) Do they protect against more than one exposure?

(b) Do they provide protection against areas with a high expected yearly loss?

(c) Do they provide protection for more than one collection of data.

(d) Will they be applicable for systems

under development as well as existing systems?

(e) Have the most cost effective protective measures been selected?

2.07 At this point in the process, it is necessary to recalculate potential yearly loss assuming the protective measure(s) have been implemented.

2.08 Next the difference between the estimated loss without protective measures implemented and with protective measures installed is calculated. From this number the cost of the protective measure(s) (from 2.05 & 2.06) is subtracted. The result is the annualized reduction of expected loss.

2.09 Using protective measure(s) cost and the estimated reduction of expected loss, a cost effectiveness ratio is calculated as the quotient; annual estimated reduction of loss divided by annual cost of protective measure(s).

2.10 The implementation of protective measures is then viewed as cost effective if the cost effectiveness ratio is greater than 1. As the cost effectiveness ratio increases the value to be gained from implementing the protective measure(s) increases.

2.11 If the total cost of the protective measure package exceeds the net effect of its implementation, (i.e. - cost effectiveness ratio less than 1), then one of the following options should be followed:

(a) Review the specific design of the proposed protective measure to determine if an alternative design can produce comparable protection at a lower cost.

(b) Restructure the data to reduce its classification and the resulting exposure, which will change the recommended level of protective measures. This might be accomplished, for example, by removing the "sensitive" data from the file, thus changing the data classification of that file.

(c) Choose a less effective protective measure package with full knowledge that adequate security may not be provided. The other two alternatives should be used whenever possible.

3.   COST-RISK ANALYSIS

3.01 The cost-risk analysis method shown for data security in subsection 2 of this section is applicable to the cost justification for the implementation of any protective measure. The important criteria to always keep in mind when performing such analysis is: "The potential savings to be gained from implementing protective measure(s) must be greater than the cost of the protective measure(s)."

3.02 The following is a brief summary of the process explained in subsection 2:

(a) Cost per loss without protective measure(s)

(b) Annual probability frequency of loss

(c) Annual loss without protective measure(s)   (A*B)

(d) Annual cost of protective measure(s)

(e) Cost per loss with protective measure(s)

(f) Annual probability frequency of loss

with protective measure(s); this
should be less than number in B

(g) Annual loss with protective
    measure(s)   (E*F)

(h) Expected reduction of loss   (C-G-D)

(i) Cost effectiveness ratio   (H/D)

4.   COST-BENEFIT ANALYSIS

4.01 Cost-risk analysis is the preferred
method to use when cost justifying pro-
tective measures for security. However,
cost risk analysis can result with very
inaccurate numbers. This occurs when the
analyst has to estimate the various costs
of associated losses. The more guesses of
costs made, the more the analysis tends to
result with invalid con-
clusions. When such a situation occurs,
formal cost-risk analysis should be aban-
doned and be replaced by a cost-benefit
analysis.

4.02 Cost-benefit analysis is not as
rigorous as cost-risk analysis. Cost-
benefit analysis tends to use a combination
of both quantitative and qualitative
methods.

4.03 Cost-benefit analysis requires the
following quantitative information:

(a) The cost of the protective measure
must be calculated. This includes
both the original development
implementation costs and ongoing
maintenance costs.

(b) The value of the data (or premises)
being protected must be assessed or
calculated. This can include the cost
to recreate the information assuming
that no other protective measures are

implemented to already assure that
such an event does not occur.

4.04 After the above information (paragraph
4.03) is calculated and verified, it is
necessary to use qualitative reasoning.
The ratio between the value of the item
protected and the cost of the protective
measure is analyzed. There are no
pre-established ratios that allow the
analyst to conclude whether or not the
protective measure should be implemented.
It, therefore, is the responsibility of the
analyst and his management to use the
information from 4.03 in a responsible
manner to conclude that the implementation
of the protective measure is or is not
justifiable.

5.   FACILITY IMPACT ANALYSIS

5.01 When trying to analyze the need and
ensuing cost justification for physical
security protective measures and/or disaster
recovery procedures, it is first necessary
to perform an impact analysis. The impact
analysis is used to determine the weak-
nesses of current security and/or recovery
systems. The analysis results are used to
determine the degree of physical security
required and to set priorities on the
recovery of specific applications.
Recommendations are then made for the imple-
mentation of protective measures. And last,
the viability of each such measure is tested
using cost-risk analysis.

5.02 Four steps are required to perform the
impact analysis. The first two steps
are designed to identify and place a value
on what needs to be protected and recovered.
The third step identifies potential threats
to the minicomputer facility and determines
current weaknesses of the physical security.
The final step recommends corrective methods
for current weaknesses based on the value

of the environment that is to be protected. Listed below is a brief summary of each of the four steps:

(a) APPLICATION EVALUATION: This is designed to evaluate the criticality of each application to the company. This can be used to create a priority list for recovering applications. Additionally, the application impact on corporate priorities is also evaluated by this step.

(b) ASSET ANALYSIS: This is designed to identify and place a monetary value on the physical assets of the minicomputer facility. The result of this step is an inventory of the physical assets and their monetary worth.

(c) PHYSICAL SECURITY EVALUATION: After it has been determined what needs to be protected, it is necessary to identify existing risks and current weaknesses. The result of this step is a list of recommended measures identified to correct the existing security weaknesses.

(d) VULNERABILITY STUDY: The final step is to determine priority of the recommended security measures based upon the impact of the applications affected and on the cost of the physical assets being protected.

5.03 After completion of all four steps, a method such as cost-risk or cost-benefit analysis should be employed to estimate the cost effectiveness of the protective measures chosen. This, in turn, determines which protective measures are implemented.

6. APPLICATION EVALUATION

6.01 The purpose of the Application Evaluation is:

(a) To determine which applications are critical and which are discretionary in the minicomputer facility and to develop an application priority list usable during a disaster recovery operation.

(b) To develop an impact evaluation of an application on company priorities (also see subsection 9), thus providing a means to determine the amount of physical security and recovery planning necessary to ensure the continued operation of the minicomputer facility.

6.02 In order to perform this evaluation, impact areas must be identified. Major areas of the company identified as being impacted by computer systems are:

(a) SERVICE: The ability to provide communication to the customer.

(b) NETWORK MAINTENANCE: The ability to maintain the integrity of the telephone network.

(c) CUSTOMER RELATIONS: The direct support of the company's ability to meet customer requirements.

(d) EMPLOYEE RELATIONS: The ability of the company to meet obligations to its employees.

(e) FINANCIAL: The ability to maintain the financial structure of the organization (normally, this area is handled on large-scale computers).

(f) OPERATIONS: The ability to maintain

the internal operation of the corporation.

(g) LEGAL OBLIGATIONS: The ability of the company to meet its legal obligations.

6.03 When evaluating the impact an application may have on the Company, additional factors must be considered. These can be used to modify the priority of an application. The following discusses these additional factors:

(a) Monetary impact of an application outage. This impact can also be of increasing negative impact to the company as an outage does not get resolved. The specific costs are associated with one of the following:

1. System Downtime Costs: This refers to the amount of time a computer facility is down. Downtime must be associated with each application particularly if multiple applications are executed on one minicomputer. The downtime must include the time to return to the point at which the system went down (includes interruption, initialization of the application, and rerun), not just the time interval of the interruption. The time can become lengthy if a large data base recovery is required.

2. Incremental Labor Cost: This concerns labor costs that are related to restoring an application after an interruption. This is limited to only identifiable, incremental, out-of-pocket expenditures. Even if employees are disrupted by the interruption but the task left undone during the downtime can be completed during

normal working hours, no incremental charges should be considered. On the other hand, if (catching up to the point where the system went down) reduction of backlog requires overtime, this should be included in the economic study. The number of people involved in an incident may be very significant. This is especially true when the incident involves distributed data processing networks.

(b) Some applications are critical at specific periods. When evaluating these applications, consider the critical processing period applicable to that application.

(c) The difficulty of reconstruction of a particular application's data base(s) could create an escalation of priority; this is referred to as recovery criticality. If this is the only factor creating a high priority, a review and redesign of the application should be considered.

(d) When determining the criticality of an application, consideration should be given to the quality of the user alternate plans for that application. If it is determined that the plans are deficient or lacking, the criticality of the application could be increased. The user should then develop alternate plans and a new review of the application should be scheduled.

(e) The impact of an application on other applications should be determined. The final priority established may then be equal to that of the most critical application affected.

7.   ASSET ANALYSIS

7.01 The first consideration to security
      planning is to identify what needs to
be protected. A dollar value is assigned
to each item that requires protection.
This entails breaking down each element in
the processing environment into a dollar
value. This provides:

(a) An inventory of all items in the
    processing environment, which is also
    usable in the event of a disaster.
    Complete information concerning
    physical plant is thus available to
    the recovery team after such an event.

(b) The dollar value of each item in the
    processing environment. This will be
    the input into the vulnerability study
    and will assist in justifying the cost
    of the recommended remedial security
    measures.

7.02 Determination of the investment in the
      physical assets of the minicomputer
facility will entail thorough and extensive
research into present in-place equipment in
each element of the processing environment.

7.03 A physical inventory of all equipment
      in each area of the processing environ-
ment specified in Section 007-590-903SW
must be recorded. This inventory should
include:

- Description of item
- Serial number
- In-place cost
- Replacement cost
- Vendor name
- Vendor contact
- Prepared order forms.

(a) On leased equipment, the following
    additional information will be
    required:

- Transportation costs
- Setup cost
- Lessor name
- Lessor contact name
- Obligation of lessee and lessor

(b) The inventory may include special
    equipment used by associated areas
    and by the user. The equipment
    should be in general proximity to the
    minicomputer facility.

7.04 Environmental control is an important
      aspect of each minicomputer facility.
An inventory of the environmental control
systems should be developed. This
inventory should contain costs as well as
capacities of each element.

7.05 The largest single investment in each
      site is the building and surrounding
area. The site investment is determined by
an inventory of the space occupied including
the building itself.

7.06 Communications is an important part
      of a clustered minicomputer facility.
Should an interruption occur, it is essen-
tial to the operations of the facility that
communication be reestablished as rapidly as
possible. Therefore, an inventory of all
communications devices should be completed
and equated to a dollar value.

7.07 Office furniture and equipment
      necessary to operate the minicomputer
center and associated areas must be
inventoried and dollar values specified.

7.08 Supplies necessary to sustain a
      complete minicomputer facility should
be recorded and evaluated. This is not a
detailed list of the number of each item,
but a list of supplies that are an
essential part of any minicomputer facility
with the average dollar investment.

Additionally, suppliers should be contacted and emergency replacement time periods firmly established.

7.09 Each application should be considered as an asset. The cost of the development or acquisition of each application within the minicomputer facility can be used to determine the value of the asset.

8. PHYSICAL SECURITY EVALUATION

8.01 Minicomputer facility security weaknesses should be evaluated and subsequent recommendations for corrective action should be made. The following paragraphs attempt to identify the areas that need investigation in order to recognize existing hazards or threats to the minicomputer facility. These threats can be divided into four categories:

(a) Natural phenomenon

(b) Design

(c) People

(d) Other

8.02 Natural phenomenon threats to the security of the facility include:

(a) Earthquakes

(b) Windstorms

(c) Floods

  - River flood plains
  - Coastal flood plains
  - Debris cones (deposited at the base of a mountain by storms).

(NOTE: Various government agencies and BSP's provide information concerning natural phenomenon threats.)

(d) Tornadoes

(e) Hurricanes

8.03 Design and geographic proximity can be a threat to a minicomputer facility. A study of the neighboring area should be conducted. Identify possible industrial hazards such as:

  - Oil fields
  - Nuclear plants
  - Airports
  - Chemical processing plants
  - High crime areas
  - Railroad main lines.

8.04 People represent the single largest risk to any computer center. This risk can be divided into two categories:

(a) Accidents which are the most common cause of problems.

(b) Deliberate acts that are potential risks to the minicomputer facility may be caused by:

  - Sabotage
  - Paramilitant groups
  - Fraud
  - Disgruntled employees
  - Arson.

8.05 Other threats include fire and power failure.

8.06 A physical security evaluation is necessary to identify the areas of vulnerability that exist in a minicomputer facility. One method of determining these vulnerabilities is through a self-examination of present security systems. One area that should be considered is the facility's general proximity to company Security Department personnel.

8.07 At the end of the evaluation, a
      summation of the present security
system should be compiled, identifying all
security problems. The corrective measures
and costs should then be determined. The
recommendations resulting from the physical
security evaluation are used as input to the
vulnerability study.

8.08 All documents associated with the
      impact analysis should be marked:

PRIVATE:
THE INFORMATION CONTAINED HEREIN
SHOULD NOT BE DISCLOSED TO
UNAUTHORIZED PERSONS. IT IS MEANT
SOLELY FOR USE BY AUTHORIZED BELL
SYSTEM EMPLOYEES.

Additionally, it should be safeguarded
according to company procedures (including
but not limited to Joint Practice 92).

9.   VULNERABILITY STUDY

9.01 The objective of this study is to
      determine implementation priority of
the recommended security measures taking
into account the associated costs deter-
mined from the physical security evaluation
and when appropriate, taking into account
the relative priority (see subsection 10)
of the individual applications executing on
the minicomputers of the facility.

9.02 Priorities should be assigned with
      the following considerations:

- The dollar value of the asset to
  be protected
- The priority of the application(s)
  within the facility
- The dollar impact of the projected
  loss of the application
- The cost of the remedial measures
  themselves

9.03 Facilities with high asset value but
      low investment must assume a priority
relative to the most critical
application(s) within the facility.

9.04 Facilities with high asset value but
      low priority applications would assume
a high priority to maintain the integrity
of the physical asset.

9.05 High-impact, low-cost security
      measures should be the first con-
sidered for implementation. Examples of
this are key control procedures and welded
hinge pins on exterior doors.

10. APPLICATION PRIORITY SPECIFICATIONS

10.01 Numerical estimates of impact are
      based on a 0 to 4 scale with the
      following interpretation:

0- DEFERRED IMPACT: Interruption of
   this application for extended
   periods will either have no impact
   or can be accomodated without
   serious penalty.

1- GENERAL IMPACT: Interruption of
   this application for up to a
   working day may cause some incon-
   venience but is an acceptable
   disruption of normal work efforts.
   The interruption will not affect
   any essential activities and will
   require only resumption of routine
   activities after termination of an
   unscheduled outage.

2- PRIORITY IMPACT: Interruption of
   this application causes moderate
   disruption of normal work effort
   for a limited group of people, has
   only minor effect on any essential
   activities, and/or requires
   reasonable time and effort to

fully restore the application
after an unscheduled outage.

3- HIGH PRIORITY IMPACT:
Interruption of this application
causes significant interruption of
normal work effort for a large
number of people, may degrade but
does not interrupt any essential
activities, and/or may require
extensive time and effort to fully
restore the application after an
outage.

4- CRITICAL IMPACT: Interruption of
this application cannot be
tolerated. Generally such
applications directly impact funda-
mental objectives of providing
service, assuring revenue, and
maintaining integrity of the core
network.

Note: Appendix 1 to BSP Section 007-590-302
contains a procedure for developing
an application recovery list.