DATA SECURITY ADMINISTRATION FOR COMPUTER SYSTEMS

COST-RISK ANALYSIS

CONTENTS PAGE

1. GENERAL

1.01 This section has been developed by a multicompany project team under the direction of the GUARDSMAN Steering Committee. This standard is being issued by the Director—Data Systems of AT&T and has been agreed to by Bell Laboratories and AT&T. Any deviation from this standard by an Operating Telephone Company is at its own risk.

1.02 Whenever this section is reissued, the reason for reissue will be listed in this paragraph.

1.03 Once data has been classified, categorized as to exposure, and appropriate types of protective measures have been selected, the next step in providing security involves a cost-risk analysis. The cost-risk analysis determines if the protective measure is cost justified. To be cost justified, the protective measure must reduce the probable annual cost of potential loss by an amount greater than the total annual ongoing costs plus the amortized development and implementation costs of the protective measures.

2. ESTIMATING PROBABLE LOSS

2.01 The first step in cost-risk analysis is to estimate the dollar value of the potential 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. Consideration should be given to the following items when making this estimation:

(a) The cost to reconstruct lost or damaged data.

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

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

(d) The costs due to loss or disclosure of revenue producing data.

(e) The cost resulting from inaccurate data affecting customer service or planning.

(f) The costs due to loss or disclosure of data which weakens our competitive position.

(g) The costs of possible legal penalties if improper information is disclosed.

2.02 The next step in the cost-risk analysis is to estimate the expected frequency of a loss. The frequency is then annualized to provide a uniform time period for comparing the probability of losses to the potential costs.

2.03 The expected yearly loss is calculated by multiplying the estimates of the cost of potential loss for each element of data by the yearly probability of loss of that respective element. The sum of these annual losses for all data represents total expected yearly loss. This loss is used as a guide for determining the amount of money which is reasonable to spend on protective measures.

3. ESTIMATING COST OF PROTECTIVE MEASURES

3.01 The costs of a protective measure 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 protection enhancements which should include such items as personnel, computer processing, storage, and system monitoring.

3.02 A protective measure whose cost is low may be selected without reference to extensive cost-risk analysis. However, a detailed cost-risk analysis must be performed for moderate to high cost protective measures. This analysis should include:

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

(b) Annual ongoing costs.

3.03 Protective measures whose costs are relatively high should be selected on the basis of how closely they meet 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?

4. PROTECTIVE MEASURE IMPLEMENTATION

4.01 Implementation of protective measures should be viewed as cost effective when the probable annual cost of potential loss has been reduced by an amount greater than the annual cost of protection plus the amortized development and implementation costs of the protective measures. This is determined by assuming that the protective measures are in place and then recalculating the annual frequency and annual probable cost per loss. This result is then subtracted from the initial probable annual cost of loss. The difference represents the effect of implementing protection and is compared with the annual cost of the protective measure. Attachment I provides an example of this methodology.

4.02 If the total cost of the protective measure package exceeds the net effect of its implementation, 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 wherever possible.

COST-RISK ANALYSIS WORKSHEET

A. Potential Loss Without Protective Measure

1. Cost per loss . . . . . _____
2. Probable frequency of loss . . . . . _____
3. Annual frequency of loss . . . . . _____
4. Annual loss . . . . . _____

B. Cost of Protective Measure

1. Initial cost . . . . . _____
2. Life expectancy of protective measure . . . . . _____
3. Amortized development and implementation costs . . . . . _____
4. Annual protective measure cost . . . . . _____

C. Potential Loss With Protective Measure Installed

1. Cost per loss . . . . . _____
2. Probable frequency of loss . . . . . _____
3. Annual frequency of loss . . . . . _____
4. Annual loss . . . . . _____

D. Cost-Risk Analysis

1. Annual loss without protective measure . . . . . _____
2. Annual loss with protective measure . . . . . _____
3. Annual expected reduction of loss (D1-D2) . . . . . _____
4. Annual cost of protective measure . . . . . _____
5. Annual expected reduction of loss (D3-D4) . . . . . _____
6. Cost effectiveness ratio (D3÷D4) . . . . . _____

COST-RISK ANALYSIS SAMPLE WORKSHEET

A.	Potential Loss Without Protective Measure	
1.	Cost per loss	$ 1,000
2.	Probable frequency of loss	Once/Month
3.	Annual frequency of loss	12
4.	Annual loss	$12,000
B.	Cost of Protective Measure	
1.	Initial cost	$ 6,000
2.	Life expectancy of protective measure	6 Years
3.	Amortized development and implementation costs	$ 1,000
4.	Annual protective measure cost	$ 2,000
C.	Potential Loss With Protective Measure Installed	
1.	Cost per loss	$ 800
2.	Probable frequency of loss	Once/Quarter
3.	Annual frequency of loss	4
4.	Annual loss	$ 3,200
D.	Cost-Risk Analysis	
1.	Annual loss without protective measure	$12,000
2.	Annual loss with protective measure	$ 3,200
3.	Annual expected reduction of loss (D1-D2)	$ 8,800
4.	Annual cost of protective measure	$ 2,000
5.	Annual expected reduction of loss (D3-D4)	$ 6,800
6.	Cost effectiveness ratio (D3÷D4)	3.2:1