Certification & Accreditation
The Risk Management Process
Dr. Bruce C. Gabrielson

Introduction

Computer security management standards and guidelines provide for the effective integration of technical, physical, and administrative measures into an overall computer and telecommunications security program. Certification and accreditation (C&A) is the means by which judgements can be made to determine the suitability of a system for controlled and secure operation in a specific environment.

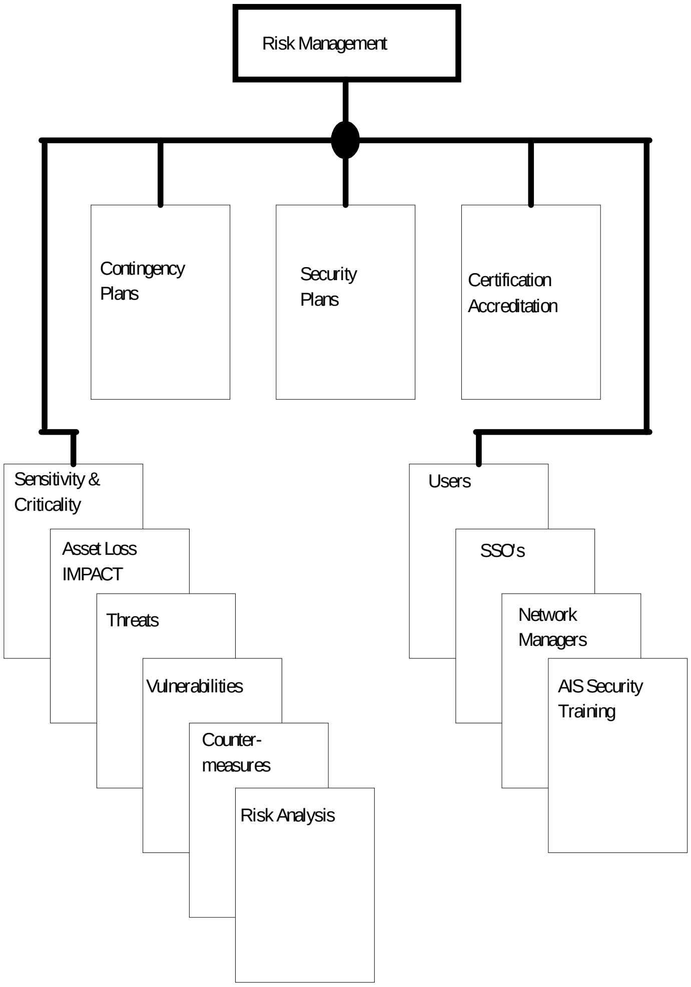
Risk Management

The risk management program, depicted in Figure 1, is an ongoing, proactive method for establishing, measuring, and maintaining an acceptable security posture for the program. It is the process through which undesirable events can be identified, measured, controlled and prevented so as to effectively minimize their impact or frequency of occurrence. This identification of the security posture forms the basis of most AIS security programs.

Risk management is a living process. Once an acceptable security posture is attained, the risk management program monitors it through everyday and follow-up activities. The risk management steps include:

1. Assign and track corrective actions, as necessary to reduce residual risk to an acceptable level.

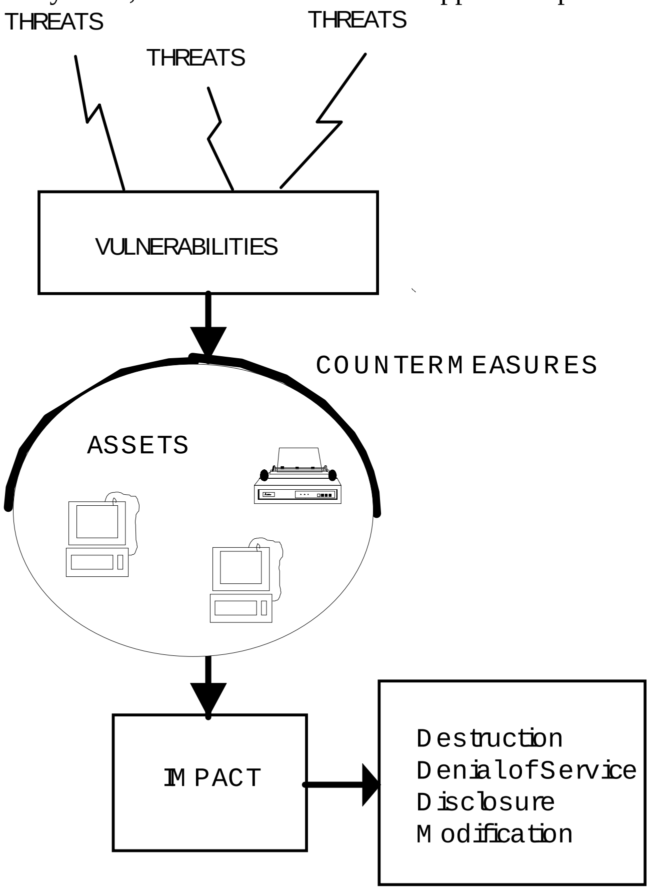
2. Continuously monitor the security posture.



Risk Analysis

Figure 2 describes the relationship between threats, vulnerabilities, countermeasures, assets, and the negative or positive impact of each. This relationship is often complicated and difficult to determine. Risk analysis is the formal process used to implement the risk management program, and is the cornerstone of the risk management process.

While risk analysis can be applied to operational systems, it is most useful when applied to prior to requirements definition of a computer application. In this way, the resulting estimates of potential loss can be used to form the basis for the computer security requirements and countermeasures being developed.



The implementation of effective information security measures must be based on a balance between the cost of controls and the need to reduce risk or expected loss using countermeasures. As shown in Figure 3, "absolute" security could be achieved only at unlimited cost.

Risk assessments are used to provide an analysis of the computer system or network assets, vulnerabilities and threats to determine the security requirements which must be satisfied to ensure the system can be operated at an acceptable level of risk. As asset's level of vulnerability to the threat population is determined solely by the countermeasures (controls/safeguards) that are in place at the time the risk analysis is done. The level of risk that remains after consideration of all in place countermeasures is called the residual risk.

Loss, which can be direct (the effort needed to reconstruct a destroyed file) and indirect (the loss or reduction of an organization's business function or cash flow due to the destroyed file) is the impact a harmful event has on the organization. Impact is usually measured in monetary values, but may also be measured in qualitative terms. The formal process of estimating potential loss is called risk analysis.

Control Measures to Reduce Potential Losses

Typical threats to computer assets are shown in Table I. Countermeasure controls often considered for implementation include:

Administrative Controls - controls include establishing policies and procedures which assign management and individual responsibilities, and conducting computer security training

Physical and Environmental - controls include limiting physical access to information resources to only authorized personnel, and protecting computers from water and fire damage, power outages, and hazardous environmental conditions

Information and Data Controls - controls include authenticating users, establishing and enforcing authorization rules for what information and processes may be accessed, and maintaining a record of user actions

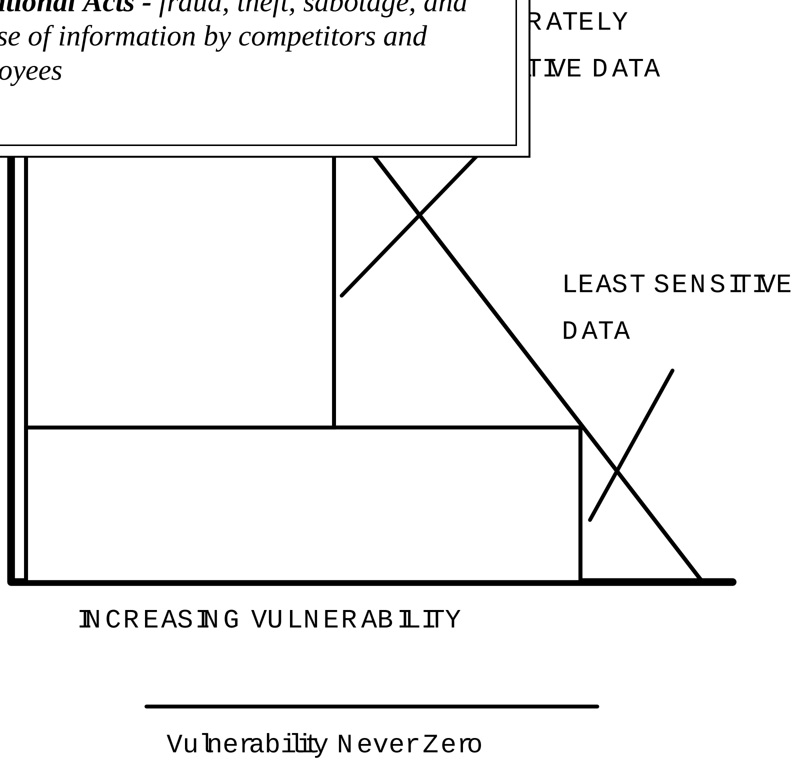
Environmental Hazards *- damage from fire, flood, dust, static electricity, or electrical storms*

Hardware and Equipment Failure - *mechanical or electrical failure of the computer, its storage capacity, or its communications devices*

Software Errors - *programming bugs to simple typos in spreadsheet formulas*

Accidents, Errors, and Omissions - *by anyone using computers or the information that they process*

Intentional Acts - *fraud, theft, sabotage, and misuse of information by competitors and employees*



Software Development and Acquisition Controls - controls include purchasing off-the-shelf software from reputable vendors, establishing rigorous controls over the development and use of programs and data for sensitive applications, and applying caution when using public domain software

Backup and Contingency Planning Controls - controls include training employees to respond to emergency conditions, maintaining backup copies of information and programs, and assuring that alternative equipment and software are available for processing if needed.

The Risk Analysis Process

Although the procedures involved in a security risk analysis are straight forward, many variations in the procedure for determining residual risk are possible[1]. Likewise, the metric for expressing residual risk can vary from good/bad or high/low to a statement that a certain amount of money will be lost. However, regardless of identifying characteristics or the figure of merit used for rating, a security risk analysis should indicate (1) the current level of risk, (2) the likely consequences, and (3) what to do about it if the residual risk is too high.

More than one technique can be used to do risk analyses. With the various techniques available, an organization should first determine what risk analysis methodology is best suited to their particular needs. Among the questions to resolve include: Which technique will produce the desired results with the least cost

[1] *DoD Directive 5200.23, CSC-S-LD-003-85, and NCSA "Rainbow Series" documents.*

and time?; Should the procedure be qualitative, quantitative, automated, manual, or some combination of these?; How many people will be needed and for how long?; How much experience must they have, what type, and what impact will their experience [or lack thereof have?; and Will the results suffer from inaccuracies or inconsistencies if not properly compiled?

Table II – Suggested Risk Analysis Report

Table of Contents
Cover sheet with report title, date, and author ID

Executive Summary

1. Introduction
   1.1 Purpose 1.2 Scope
   1.3 Background
2. System Description
   2.1 Overview
   2.2 Hardware
   2.3 Software
   2.4 Communications: Network Environment
   2.5 Sensitivity
   2.6 Criticality
3 Methodology Used
   3.1 Data collection
   3.2 Data analysis
   3.3 Reporting and risk management
4. Conclusions
   4.1 High vulnerability areas
   4.2 Significant threats
   4.3 Measure of compliance (required cm's)
   4.4 Most significant vulnerability(ies) due to paired threats
5. Recommendations
   5.1 Rationale

Risk Analysis Steps

There are several basic steps to doing a security risk analysis. The amount of effort involved with each will vary greatly based on the size and complexity of the "system" being analyzed.

The first step is often critical in that the scope of the system needs to be accurately defined. Most important is the determination of where the system starts and ends and what components (individual computer systems, networks, etc.) are included in the definition of the "system."

The results of the analysis are compared against a predetermined figure of merit to determine if additional countermeasures are necessary. Some guidelines exist for establishing figures of merit (see Attachment A to this section), but asset cost is normally the determining factor. However, many organizations simply rely on those incorporated into available automated risk analysis software. Existing countermeasures should be systematically evaluated and compared against the figure of merit selected to ensure they are both necessary and properly implemented. Figure 4 describes the evaluation flow for countermeasure evaluation.

Risk Analysis Steps
1. Identify what needs to be protected (assets)
2. Identify what to protect from (threats)
3. Identify safeguards in-place (countermeasures)
4. Identify weaknesses (vulnerabilities)
5. Determine estimated loss due to threats (expected loss)
6. Recommend corrective action(s)

What Should The Risk Analysis Report(s) Show?

Table II provides an example of a suggested security risk analysis report format. The biggest challenge in writing a security risk analysis report is to bridge the gap between risk analysis jargon and information management can understand and use for decision making. As a rule, management will focus on summary information and only use technical details if they are needed to support a decision or make a choice between recommendations.

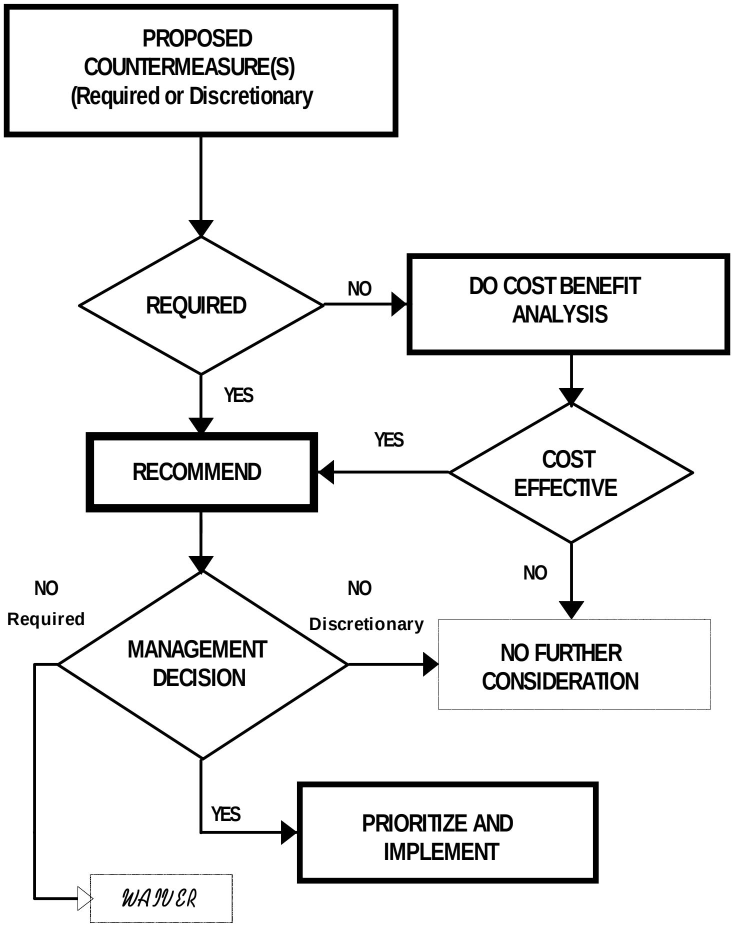
Those technical details should include, as a minimum:

1. Vulnerability levels
2. Applicable threats and their frequency
3. The use environment
4. System connectivity
5. Data sensitivity level(s)
5. Residual risk, expressed as:

Qualitative?
Quantitative?

Manual Verses Automated Methods

The most basic function of any security risk analysis process is to determine, as accurately as possible, the risk to assets. Of course, the procedure for determining the risk can be complex or simple, depending on the asset and on the analysis methodology used. The amount of risk can be expressed as good/bad; high/low (qualitative), as a calculated metric (quantitative), or a combination of the two (hybrid).



The process of data collection, analysis, and preparing a security risk analysis report involves many steps. It is time consuming, expensive, and more often than not, a collateral duty for the person(s) charged with getting it done. Moreover, the requirement to do a security risk analysis is cyclic in nature, e.g., initially, then once every three years.

Which methodology for security risk analysis is best; qualitative?, quantitative?, or hybrid? Should the process be manual or automated? There is little doubt that an automated risk analysis methodology is less demanding on the user in terms of time and experience. The concepts and implementation of most commercial automated methodologies have undergone the scrutiny of both government and commercial users.

In contrast, manual methods are often less formal and require the user to interpret and execute numerous, and sometimes complicated, steps. This increases the likelihood of error or omission and makes repeatable results difficult to obtain.

Audit and Evaluation

Once the initial risk analysis is performed and the security program is in place, other parts of the risk management program come into play. Because security requirements should be a consideration throughout the entire life cycle of a system, security measures are best when designed into systems from the start. Steps should be taken to assure that planned security mechanisms are implemented and working as intended. Effective processes for audit recording and review security should be in place to ensure accountability and to provide a means of monitoring potential threats to operational systems.

System Test and Evaluation (ST&E)

The ST&E function is the active auditing part of the ADP security configuration management procedure. ST&Es gather empirical data on individual systems and are examined by the DAA in the evaluation procedure. This process evaluates the effectiveness of in-place countermeasures against incidents that would effect the AIS in a negative manner. If the in-place countermeasures are inadequate, the ST&E will uncover this fact and they can then be rectified.

Contingency Planning

Since computers and networks fail, often leaving user's unable to accomplish critical processing, guidance is needed to assist users and managers in providing effective contingency planning. Effective planning and operational procedures to assure that critical applications and data are available in a timely manner.

Specifics of a Typical C&A Program

Risk assessments, system test and evaluation, and contingency planning are all parts of the risk management program. The certification and accreditation process provides the formal management authorization procedure to implement the program. By ascertaining what level of risk is acceptable for an individual system, the accreditation team can determine which countermeasures are necessary in maintaining the level of security required over the life-cycle of the AIS. The formal investigative process (shown in Figure 5) involves the data collection and analysis (risk analysis) of the system's exposure to risk using a risk assessment as previously described.

Accreditation

The accreditation of a system by the ADP security office for use in classified or unclassified but sensitive processing certifies that the system examined is configured in compliance with relevant security compliance guidelines. Using the risk management approach, the ADP Security Office considers Risk Analysis (RA), Contingency Planning (CP) and Security Test & Evaluation (ST&E) for each AIS. Risk Management is an ongoing process that will periodically reaffirm the validity of the previous accreditation throughout the life of the AIS. The AIS Security Officer supports the risk management program by performing the following tasks:

1. Development and maintenance of the accreditation schedule.

2. Perform a risk assessment and analysis by analyzing threats to the AIS and vulnerabilities to the AIS in relationship to the sensitivity of the data processed by the AIS.

3. Ensure a contingency plan is in place for the continuity of operations in an emergency situation and that the developed plans are exercised.

4. Ensure that required countermeasures are implemented.

5. Ensure that security tests, TEMPEST tests, and other inspections are conducted as required.

6. Perform technical review for security-related waiver requests.

Typical Procedures

When the user decides to purchase a new AIS system, he must fill out several forms. The form that concerns our office is the ADP System Accreditation Request form. By completing this form and sending it to our office, you are granted interim accreditation that lasts until our office can initiate a field risk assessment which will result in final accreditation of the system within 90 days of the examination.

TEMPEST Vulnerability Assessment Request Form (TVAR)

The TVAR form is filled out by the user after the final accreditation process in order to assess whether emanations that may be present are at risk of being transmitted.

Interview Process

The interview process is initiated when an AIS is being processed for final accreditation. An interview is conducted with the designated custodian for a system, and a questionnaire is normally completed. This process supports the on site evaluation of a system.

Interim Accreditation

Interim accreditation is granted as soon as the ADP system accreditation request form is processed. This accreditation is normally valid for a pre-specified period of time or indefinitely until an on-site evaluation can be scheduled. This type of temporary accreditation carries with it the authority to operate at the level of classification that was requested.

Physical Access Control (Area Control)

Physical safeguards for AISs are necessary to minimize the potential for problems caused by certain threats. The level of physical protection is directly related to the sensitivity and cost of the AIS. These are the minimum requirements for physical safeguards for each of the data level categories. There may be instances where the minimum is not enough protection, but in general, the following physical requirements should be followed when planning for and/or installing AISs, Networks and computer resources.

CONTINGENCY PLANNING

The backup plan to be used in the event of an emergency.

Provides for efficiently returning lab AIS to full productivity after an interruption.

CONTINGENCY PLAN ITEMS

Emergency Response Team List
Secure Storage Site
Complete Archive Backup
Current Incremental Data Backups
Testing Conditions

Contingency Management

Contingency Management is an essential continuity provision incorporated into the ADP security process. It provides the user with a backup plan in the event of an emergency involving the temporary incapacitation of the system. This would prevent loss of vital data, time spent trying to organize directly after the event occurs, and interruptions of the work process that would cost precious time and money.

Certification

Once all requirements for accreditation have been complied with, formal accreditation for the evaluated system is provided. Unless there is a major modification, the accreditation will be reviewed every three years, and will remain in effect until the machine is no longer used for classified processing. However, if the AIS is to be replaced or surplussed, the security office must be notified so it can be removed from the approved systems database.

CERTIFICATION

A comprehensive Assessment of the evaluation, risk assessment, and security plans to determine is the AIS meets applicable requirements

Computer Security Training and Awareness

For AISs which process classified information;, proper training and awareness for the user are key integrity factors as well as being mandated by Government regulations. Awareness by the end-user of good security techniques can and does cut down on security incidents, especially when the AIS is networked. Security starts with the custodian of the machine, and he or she must be responsible for all user actions.

Appendix A

5200.28 (Encl 4)

PROCEDURE FOR DETERMINING MINIMUM AIS COMPUTER-BASED SECURITY REQUIREMENTS

A. RISK ASSESSMENT PROCEDURE. The following risk assessment procedure is extracted from CSC-S-LD-003-85 (reference (u)). The procedure is used to determine the minimum evaluation class required for an AIS, based on the sensitivity of the information present in the AIS and on the clearances of its users. Any DoD Component desiring to use a different method to accomplish the intent of,this enclosure may do so, if prior approval has been granted by the ASD(C3I).

> NOTE: In the case of a network, the procedure is applied individually to each of the AISs in the network. The resulting evaluation class should be taken as a minimum partial requirement since connection of an AIS to another AIS or to a network may result in additional risks (see enclosure 5). The DAA for a network also may decide to apply the procedure once for the network, and determine the evaluation class by applying the requirements in DoD 5200.28-sc (reference (k)) to the network as a whole.

1. Step 1. Determine System Security Mode of Operation. The system security mode of operation for an AIS is determined as follows:

> a. An AIS is defined as operating in the dedicated security mode if all users have the clearance or authorization, documented formal access approval, if required, and the need-to-know for all information handled by the AIS. The AIS may handle a single classification level and/or category of information or a range of classification levels and/or categories. The AIS shall be isolated electrically, logically, and physically from all personnel and AISs not possessing the requisite clearance or authorization, formal access approval, if required, and need-to-know for all of the information handled by the AIS.
>
> b. An AIS is defined as operating in the system high security mode if all users have the clearance or authorization and documented formal access approval, if required, but not necessarily the need-to-know for all information handled by the AIS.
>
> c. An AIS is defined as operating in the multilevel security mode if not all users have the clearance, authorization, or formal access approval, i.f required, for all information handled by the AIS.
>
> d. An AIS is defined as operating in the partitioned security mode if all users possess the clearance, but not necessarily a formal access approval, for all information handled by the AIS.

2. Step 2. Determine Minimum User Clearance or Authorization Rating. The minimum user clearance or authorization (Rmin) is defined as the maximum clearance or authorization of the least cleared or authorized user. Rmin is determined from Table 1. The clearances used in the following table are defined in DoD Directive 5200.2 (reference (p)).

Table 1
MINIMUM USER CLEARANCE OR AUTHORIZATION SCALE

	Rating
Uncleared OR Not Authorized (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified Information (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS) and/or Current Background Investigation (BI)	4
TS and/or Current Special Background Investigation (SBI)	5
One Category (lC)	6
Multiple Categories (MC)	7

3. Step 3. Determine Maximum Data Sensitivity Rating. The maximum data sensitivity (Rmax) is determined from the following table:

Table 2
MAXIMUM DATA SENSITIVITY SCALE

Maximum Sensitivity Ratings 2/ Without Categories (Rmax)	Rating (R)	Maximum Data Sensitivity With Categories 1/	Rating (Rmax)
Unclassified (U)	0	Not Applicable 3/	
Not Classified but Sensitive 4/	1	N With One or More Categories	2
Confidential (C)	2	C With One or More Categories	3
Secret (S)	3	S With One or More Categories With No More Than One Category Containing Secret Data	4
S		With Two or More Categories Containing Secret Data	5
Top Secret (TS)	55/	TS With One or More Categories With No More Than One Category Containing Secret or Top Secret Data	6
		TS With Two or More Categories Containing Secret or Top Secret Data	7

1/ The only categories of concern are those for which some users are not authorized access. When counting the number of categories, count all categories regardless of the sensitivity level associated with the data. If a category is associated with more than one sensitivity level, it is only counted at the highest level. Systems in which all data is in the same category are treated as without categories.

2/ Where the number of categories is large or where a highly sensitive category is involved, a higher rating might be warranted.

3/ Unclassified data by definition may not contain categories.

4/ Examples of N data include financial, proprietary, privacy, and mission sensitive data. In some situations (e.g., those involving extremely large financial sums or critical mission-sensitive data), a higher rating may be warranted. Table 2 prescribes minimum ratings.

5/ The rating increment between the Secret and Top Secret data sensitivity levels is greater than the increment between other adjacent levels. This difference derives from the fact that the loss of Top Secret data causes EXCEPTIONALLY GRAVE damage to U.S. national security, whereas the loss of Secret data causes SERIOUS damage.

4. Step 4. Determine Risk Index. The risk index depends on the rating associated with the AIS minimum user clearance (Rmin) and the rating associated with the maximum classification of the information handled by the AIS (Rmax).

The risk index is computed as follows:

a. Case a. If Rmin is less than Rmax, then the risk index is determined by subtracting Rmin from Rmax.

Risk Index = Rmax - Rmin

NOTE: There is one anomalous value that results because there are two "types" of Top Secret clearance and only one "type" of Top Secret data. When the minimum user clearance is TS/BI and the maximum data sensitivity is Top Secret without categories, then the risk index is 0 (rather than the value 1, which should result from a straight application of the formula).

b. Case b. If Rmin is greater than or equal to Rmax, then:

Risk Index = 1, if there are categories to which some users are not authorized access, or:

Risk Index = 0, ia all other cases.

5. Step 5. Determine Minimum Security Evaluation Class For Computer-Based Controls.

a. The following table shall be used to determine the minimum security class required for an AIS based on the computed risk index in Step 4, above. The levels in the table are those described in DoD 5200.28-STD (reference (k)).

Table 3
COMPUTER SECURITY REQUIREMENTS SCALE

Risk Index	Security Mode	Minimum Security Class 4/
0	Dedicated 5/	No minimum class I/, 2/
0	System High	C2 2/
1	Multilevel, Partitioned	B1 3/
2	Multilevel, Partitioned	B2
3	Multilevel	B3
4	Multilevel	Al
5	Multilevel	
6	Multilevel	
7	Multilevel	

1/ Although there is no prescribed-minimum class, the integrity and denial of service requirements of many systems warrants at least class C1 protection.

2/ Automated markings on output must not be relied on to be accurate unless at least class, B1 is used. (See requirements for marking in enclosure 3.)

3/ Where an AIS handles classified or compartmented data and some users do not have at least a Confidential clearance, or when there are more than two types of compartmented information being handled, at least a class B2 is required.

4/ The asterisk (*) indicates that computer protection for environments with that risk index is considered to be beyond the state of current computer security technology.

5/ Most embedded systems and desk top computers operate in the dedicated mode.

6. Step 6. Adjustments to Computed Security Evaluation Class Required. Additional requirements or recommendations relevant to determining the minimum evaluation class include the following:

a. Where an AIS is connected to a network or to another AIS, care should be taken to ensure that the requirements for accreditation of the AIS are not violated due to the presence of the network technology.

b. In the dedicated mode where the AIS is connected to a network or to another AIS, it is recommended (although not required) that at least level C1 be used. This recommendation is made because level C1 might provide a measure of security sufficient to prevent users from accidentally altering or deleting each other's data.

c. An AIS using periods processing (i.e., operating in one or more security modes and/or at one or more security levels for certain periods of time where acceptable sanitization procedures are implemented between processing periods) may have more than one risk index. In such cases, the highest value of risk-index shall be used in determining the minimum security feature level.