Chapter 8

Certification & Accreditation
The Risk Management Process

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 judgments can be made to determine the suitability of a system for controlled and secure operation in a specific environment.

DOD AIS ASSURANCE

DOD Directive 5200.28
Risk Management Program
Accreditation
Risk Analysis
Contingency Planning
Security Test & Evaluation

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.

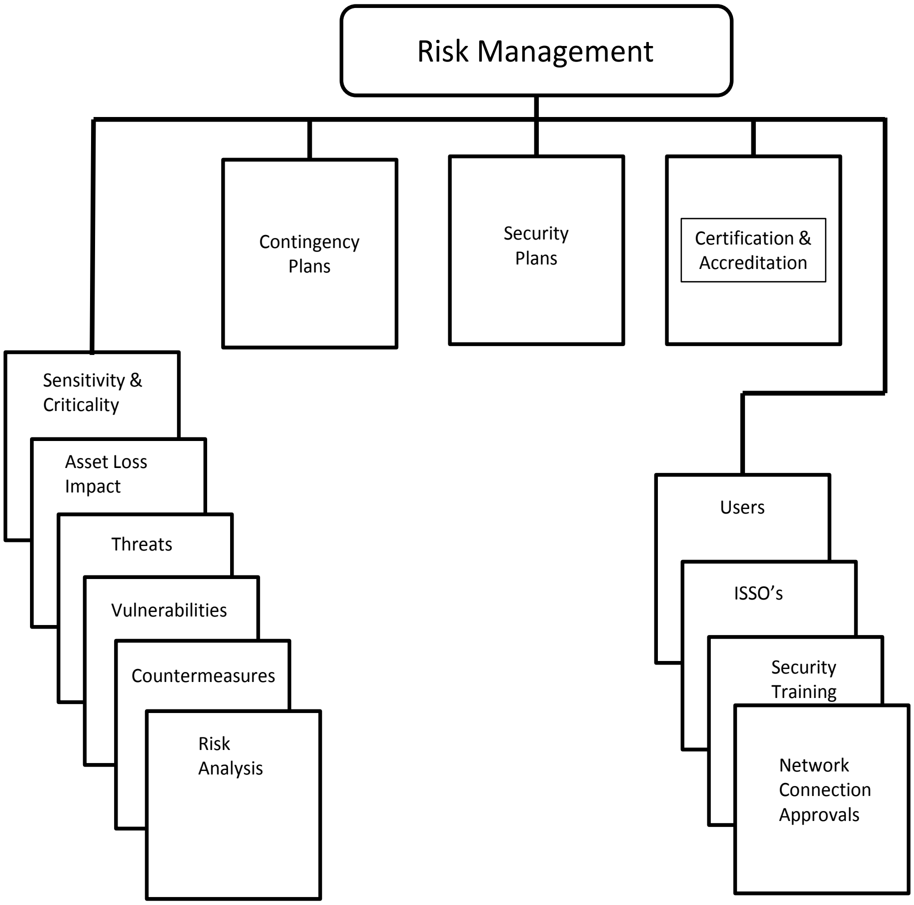

Figure 1 - Risk Management Program

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

1. Assign and track corrective actions, as necessary to reduce residual risk to an acceptable level.
2. Continuously monitor the security posture.

RISK MANAGEMENT

The implementation program for AIS security is known as Risk Management.

Risk Management assures an activity's mission can be carried out while reducing computer security risk to an acceptable level.

Risk Management weighs the costs of security against the gains in actual protection.

Decides what must be protected, what it must be protected from, and how to protect it.

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.

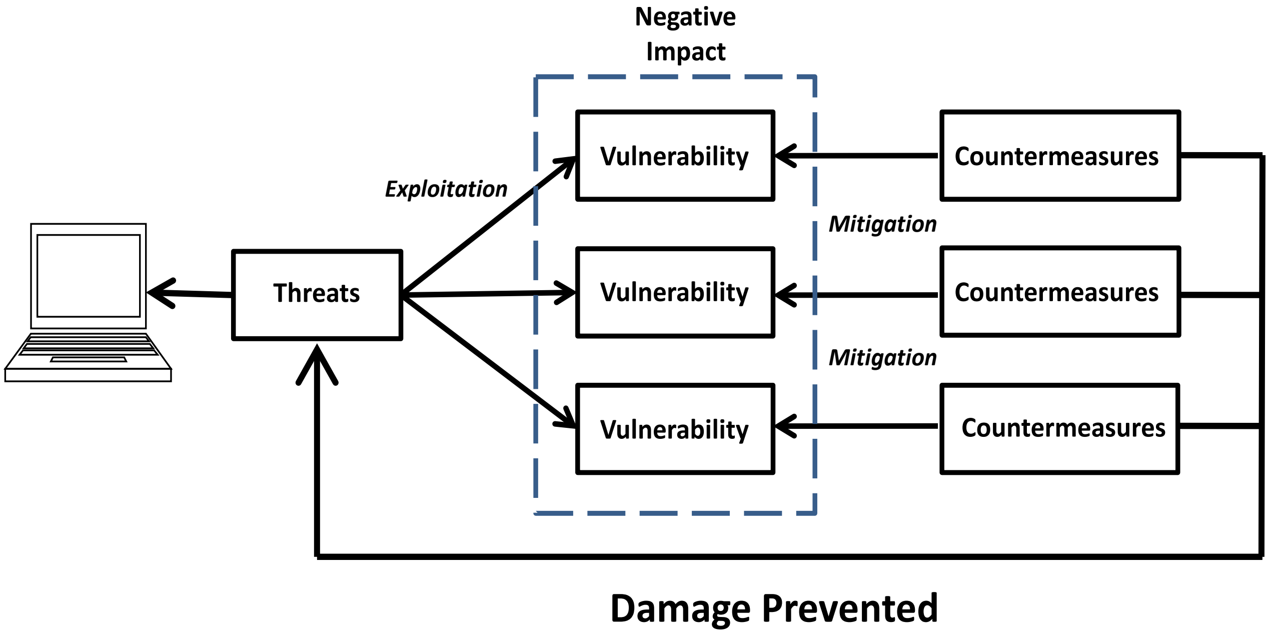

Figure 2 – Threat/Vulnerability/Countermeasure Model

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.

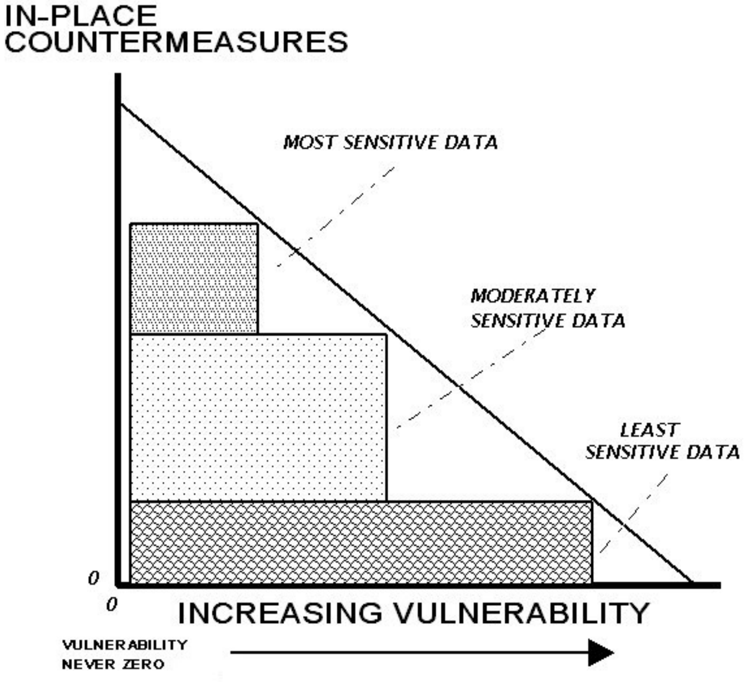

Figure 3 – The Countermeasures vs. Vulnerability Dilemma

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 and/or 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.

COUNTERMEASURES

Risk (Cost Trade-Off) Analysis
Initial Cost
Periodic Re-Evaluation

TEMPEST Vulnerability Assessment
Suppressed Equipment
Radiation Zone

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.
- **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

- **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 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?

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."

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)***

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

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

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.

What Should The Risk Analysis Report(s) Show?

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.

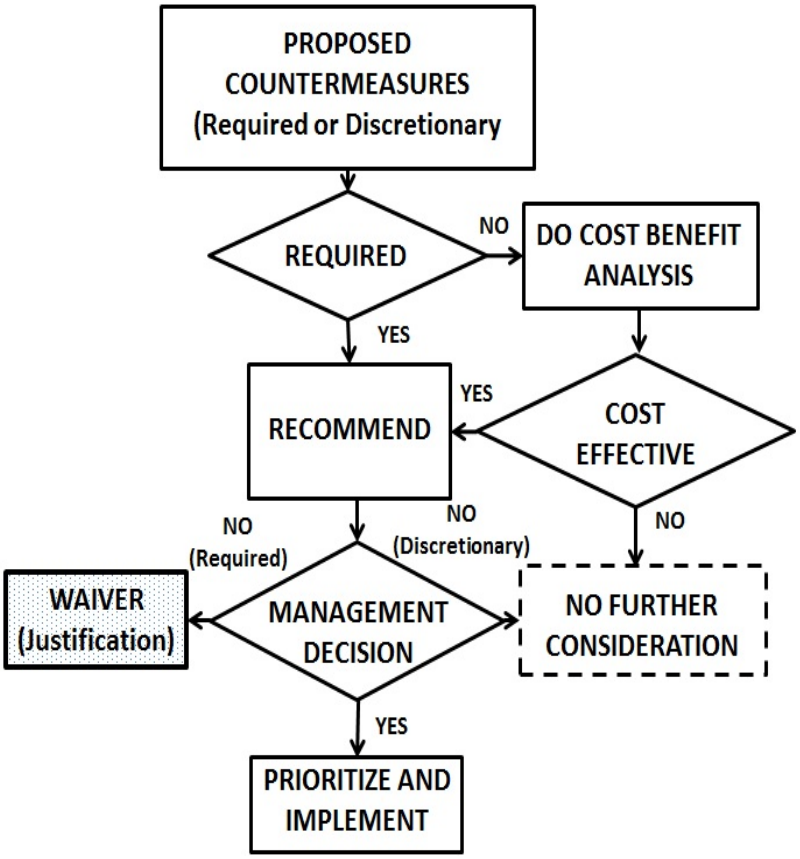

Figure 4 – Evaluating Countermeasures

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 impact 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.

ST&E

ST&E is the active auditing part of a comprehensive ADP security procedure.

Process evaluates the effectiveness of in-place countermeasures against incidents that would impact the AIS in a negative manner.

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 assure that critical applications and

NETWORK TESTING

Most thorough organizations actively test their networks to both in-place protective measures and unauthorized use.

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 PROCESS

User Responsibility
ADP System Request Form
TVAR

Areas Evaluated
Equipment Type and Configuration
Operating Procedures
Physical Access Control
Contingency Management

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

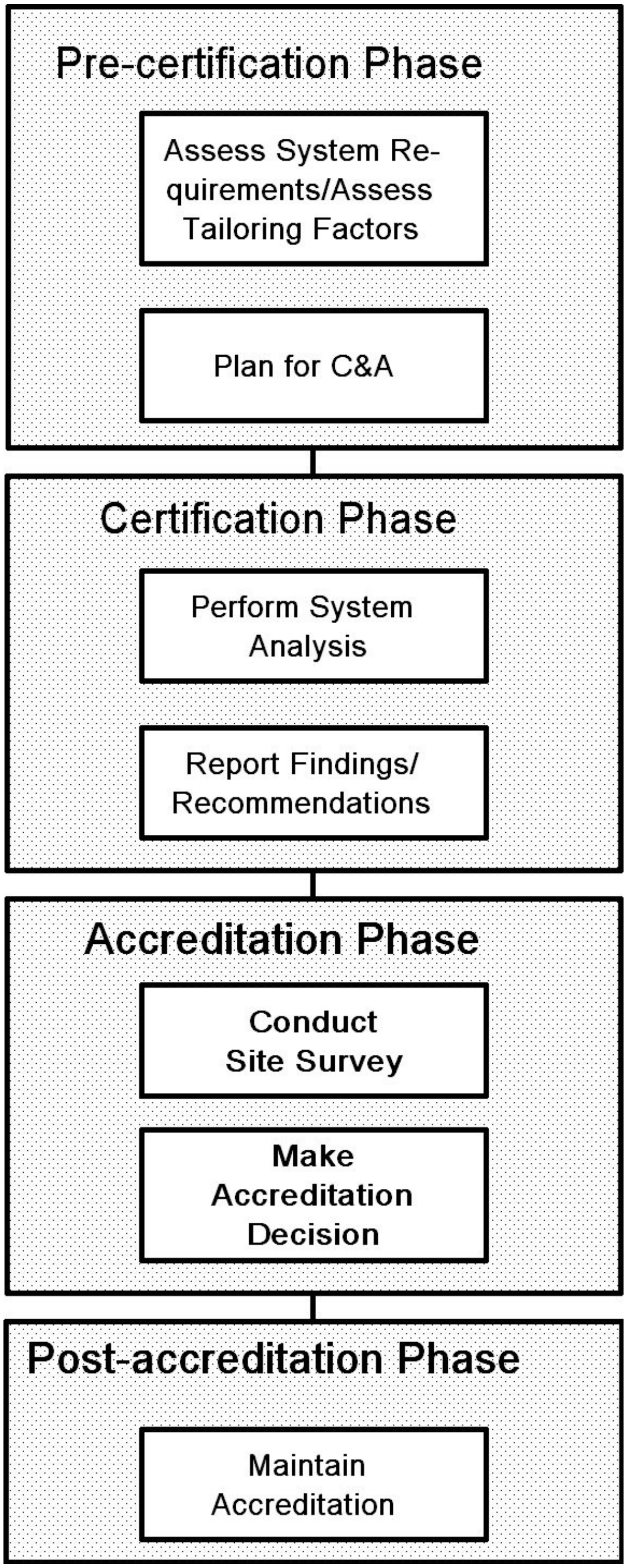

Figure 5 – C&A Process

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.

STEPS TO ACCREDIT AN AIS

System Accreditation Request application submission

Interim Accreditation granted by ADP Security Office until evaluation can be scheduled

Physical Access Control (Area Control) establishment

Contingency Management plan development for emergency backup

Formal Accreditation (Certification)

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.

POSSIBLE ACCESS CONTROLS

- ***Signs, locked doors, cipher locks***
- ***ID cards and/or badges***
- ***Access log***
- ***Closed-circuit TV***
- ***No unauthorized unescorted entry***

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.

CONTINGENCY PLAN ITEMS

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

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 surplused, the security office must be notified so it can be removed from the approved systems database.

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.