An Accrediting Official or group of Officials might be responsible for several applications, but for each application, there is typically only one Accrediting Official or group of Officials assigned. For example, some Department of Defense (DoD) applications require more than one Accrediting Official. This occurs because several DoD agencies serve as custodians for particular types of information and each must approve the security safeguards of applications that process this information.

Where privacy is a concern, Federal managers can be held personally liable for security inadequacies. The issuing of the accreditation statement fixes security responsibility, thus making explicit a responsibility that might otherwise be implicit. It also shows that due care has been taken for security. Accreditors should consult the agency general counsel to determine their personal security liabilities.

1.3.2 Certification Program Manager

The Certification Program Manager is responsible for defining and managing the security certification program within an agency. While the details of this role might vary widely, at a minimum it involves producing agency specific certification guidance and periodically reporting to management on program status. It might also involve active oversight of certifications. (See Appendix G for an example that enumerates a possible set of responsibilities.)

There is typically one Certification Program Manager designated within an agency. If the agency includes somewhat autonomous subsidiary components, such as the Public Health Service or the Social Security Administration within the Department of Health and Human Services, these components might also have individuals designated to manage the component certification programs. The role of Certification Program Manager can be assigned to the Agency ADP Security Officer. It might also, along with the security officer role, be assigned to the Information Resources Management office.

The individual selected to fill this role should possess substantial knowledge of agency structure, politics, agency program, mission objectives, and capabilities as well as general knowledge of ADP and security. The role is that of a management professional rather than a technical analyst.

1.3.3 Application Certification Manager

The Application Certification Manager is responsible for managing a specific certification effort. This individual plans the effort, procures evaluation resources, and oversees production of the security evaluation report. The person selected as Application Certification Manager is as independent as possible from the application being certified, to help ensure an objective evaluation. Ideally this person is familiar with the application requirements and technology, as well as generally-accepted computer security safeguards. (See Appendix G for an example that enumerates a possible set of responsibilities.)

In some cases, several certification efforts are performed in support of one accreditation decision. This can arise due to the partitioning of organizational responsibilities into several technical security areas. In such cases, it is preferable to integrate the technical certification findings into one final report, since the safeguards in each area can have complex interrelationships that require a technical interpretation.

1.3.4 Security Evaluator

Security Evaluators perform the technical security evaluation tasks. Their responsibility is to provide expert technical judgments in their areas of specialization. Required Security Evaluator specializations vary with each application. For basic (high-level) evaluations, computer security generalists with some application-specific training are sufficient. For detailed evaluations, greater specialization is required. Useful specialties include: application analysts, systems analysts, engineers, designers, application programmers, systems programmers, testers, contract specialists, and lawyers. For detailed developmental certifications, Security Evaluator skill requirements vary with the developmental phases, as shown in Appendix F. Security evaluation is typically best performed by a team, since this provides the advantage of combined skills and viewpoints.

As implied above, Security Evaluators are as independent as possible from the application. Nevertheless, while security evaluation requires a degree of independence to help ensure objectivity, a fully independent evaluation is not feasible in many cases. In some areas it is necessary and reasonable to accept the technical judgments of application developers and users. Furthermore, every application has people associated with it who are already aware of many of its flaws. For example, system programmers are usually aware of operating system shortcomings. While these people might not have the authority or resources to correct deficiencies, their expertise should be sought in identifying the deficiencies. The Application Certification Manager must weigh the benefits of independence against its increased expense, and arrive at an appropriate mix.

1.3.5 **Responsibilities Of Agency Offices**

Many agency offices should support the certification program. It is especially important that offices associated with the application being evaluated cooperate with and support certification efforts. They must provide briefings, interviews, and documentation as requested. They might be required to prepare application flow charts and control listings and to complete questionnaires or checklists. They might also be required to assist in the preparation of security requirements and risk analyses. They should also be responsible for informing appropriate authorities on the initiation of a development effort and on the occurrence of events such as violations or errors in operational applications that might require or affect certification. It is useful to assign an application person as the point-of-contact for the certification team.

Primary support from other offices is through the loan of personnel to provide security evaluation support or, where this is not possible, through the direct performance of evaluation tasks for the certification effort. Agency review offices such as the ADP portion of the Office of the Inspector General (OIG), ADP Security Office, ADP quality assurance and standards, and test and evaluation are key providers of independent technical evaluation support. Some of their own internal work also provides certification evidence. The major example is the evaluation of application compliance with internal security-relevant policies or standards that were formulated by these offices (e.g., audit requirements, developmental standards, measures-of-test-coverage standards). For the most cost effective security evaluation support, quality assurance and VV&T (Validation, Verification, and Testing) should be provided for in the planning phase of an application's development.

It is important to distinguish between the certification and accreditation program and the duties of the OIG. Auditors do not serve as Accrediting Officials, since this would impair the auditors' independence. The auditors' main certification support responsibilities are: (1) to provide technical evaluation, as required, in assessing control adequacy and auditability and (2) to inform appropriate authorities of situations that might require or affect certifications. Auditors often obtain certification relevant findings which should be forwarded to certification program personnel.

1.4 Considerations for Scheduling

Certification and accreditation can be performed on applications that are operational or under development. For several reasons, it is preferable to perform initial certification and accreditation when an application is under development. First, it is easier to change an application under development than one that has been in operation for a period of time. Second, it is easier to prevent a severely flawed application from becoming operational than to remove it from an operational state. A number of factors underlie this.

1. *Resistance to change.* People resist change. This is true of changes to any operational system but can be especially applicable in security relevant cases, since the change might add procedural steps, restrict existing capabilities, restrict flexibility, increase application response time, or remove capabilities previously present. There is resistance to change during development, also, but the amount of resistance is usually less since there is no large entrenched constituency.

2. *Costs.* Financial and technical resources required to make security changes to an operational application are far greater than those required to make similar changes during development. Some estimates place the costs for changes during operation as being at least thirty times higher [GA082-1, p. 29].

3. *Lack of exploitation evidence.* It might be difficult to justify the correction of even a major flaw if an application has been operational for years without evidence of the flaw being exploited. Sometimes the absence of exploitation evidence might indeed be valid "proof" that the threat is not sufficient to warrant increased safeguards. The lack of evidence, however, does not ensure that the flaw is not being or will not be exploited. In addition, many computer security flaws are such that even one exploitation could have disastrous effects. This is especially true in the contingency planning area [FIPS87].

Another reason for performing certification and accreditation during development is that it permits the development process itself to be changed. For example, if certification analysis shows development quality to be insufficient, strict programming standards can be adopted. Developers might be requested to provide evidence of security analysis.

It is worth emphasizing that the above arguments can be overridden. The most important criterion in deciding which certifications and accreditations to perform first is application sensitivity (as might be reflected in a prioritized listing of agency applications by sensitivity). If the greatest sensitivity is possessed by an operational application, it should generally be the first to be examined. Even here, however, there are other factors to consider. For example, certification of a low sensitivity application might be scheduled before certification of a high sensitivity one in order to acquire needed training and increase technical proficiency. The point here is that, though situational needs must be considered, it is usually best to initially certify and accredit applications while they are under development. This is in keeping with the principles of life cycle management, and ensures that major certification influence occurs during the "formative" period in an application's life. Appendix F shows how certification and accreditation activities are interleaved with application development.

1.5 Evaluation Techniques for Security Certification

Evaluation of computer security is an activity that has slowly been growing in importance and is performed in four communities affected by computer security issues. These communities are the ones that perform: 1) risk analysis, 2) validation, verification, and testing (VV&T), 3) security safeguard evaluation, and 4) EDP audit. Each of these communities has many approaches to evaluation of security and performs these evaluations for different purposes. A security evaluation performed for certification is characterized by using security requirements as criteria or the baseline for evaluation. When any one of the above communities uses security requirements as criteria for evaluation, their evaluation can be used for certification.

Evaluation for certification involves validating security requirements, examining safeguards or controls, and determining whether safeguards satisfy requirements. Primary emphasis is on requirements and safeguards rather than on threats, assets, and expected losses. Methods of evaluation used in each of the four communities cited above can be adapted for use as evaluations for certification. The integration of these adapted methods into the certification process described in this Guideline is a large component of this computer security technique named "certification and accreditation."

A certification begins by reviewing the requirements for acceptability. In areas where threats and expected losses are well understood, risk analysis methods can be used. Where threats and expected losses are not well understood, evaluation aids for certification such as security checklists or control reviews can be used. The objectives of this type review are summarized in Section 2.3.1. Security safeguard evaluations and EDP audit methods can be used to select additional security requirements when the evaluation used for certification finds the application lacking in some area.

If no security requirements have been explicitly formulated when certification begins, the certification team must come up with such a formulation in order to perform an evaluation for certification. Risk analysis data can be used for this purpose.

As the application development process unfolds in the application life cycle, the certification process determines whether controls satisfy security requirements, and does this at different levels of specificity. As described in Section 2.3, the minimum level of evaluation for certification is a 'basic evaluation' and includes reviewing the functional specifications against security requirements. For areas of the application that need in-depth security assessment, a 'detailed evaluation' is performed, as described in Section 2.4. As appropriate, the various groups of security evaluation methods are called upon to provide these reviews.

During the operation and maintenance of the application, recertification and reaccreditation will eventually be needed. This means that an evaluation for recertification must occur. Recertification evaluation is similar to a certification evaluation but takes place more selectively since areas of the application that experience no changes need no action. Note that an operational application that has never been certified is a candidate for certification, not recertification.

The following briefly describes and compares the four groups of security evaluation methods that can be used for certification evaluation.

1.5.1 Risk Analysis

1.5.1.1 Its Uses—The primary purpose of risk analysis is to understand the security problem by identifying security risks, determining their magnitude, and identifying areas where safeguards or controls are needed. It can also be used to determine how many resources to budget for security and where to allocate these resources. It is best performed at the beginning of the system life cycle and, with user inputs and policy requirements, can provide the basis for choosing system security requirements (Phase I in fig. 1-1).

Risk analysis can also be useful in validating requirements (Phase IIA in fig. 1-1). If requirements are defined to the functional safeguards level, risk analysis can be used to determine whether the protection embodied in the controls reduces expected loss to an acceptable level at acceptable cost (Phase IIB in fig. 1-1). This is typically done by estimating reduced threat frequencies or damages based on the presumed implementation of the identified safeguards. Risk analysis thus plays a dual role in any certification program because it can be used both to help determine important security requirements (the criteria for the process of certification) and to evaluate the safeguards.

Some further things to note about risk analysis are: (1) risk analysis is a stand-alone process that can be performed independently of a certification; (2) it is usually performed under the direction of people internal to the system in question; and (3) risk analysis becomes an evaluation technique for certification when a particular level of loss becomes an acceptable security requirement of the application. Figure 1-1 shows the relation of certification and risk analysis to the application's life cycle. For examples of risk analysis methods see [FIPS65], [SDC79], [IST79], and [HOF80]. For a discussion of risk analysis methods and brief descriptions of them see [NBS83]. Note that [OMB78] requires risk analysis as well as certification for sensitive applications.

1.5.1.2 Its Limitations—Theoretically, risk analysis can be used to examine the effectiveness of any control by determining its impact on expected loss. This holds true in areas such as environmental security, where reliable data exist on threats such as fires and floods and the losses they might cause. In situations where reliable data do not exist on threat frequencies and expected losses, it is extremely difficult to evaluate safeguards in such terms and so accuracy of the findings diminish. For example, it is difficult to determine whether and to what extent the addition of a software safeguard will reduce the threat from a system penetrator. Similarly, although the addition of authentication safeguards reduces expected losses from unauthorized access, it is difficult to specify the extent of this reduction. This reduced accuracy applies not only to analyzing less understood controls but also to analyzing technically detailed safeguards such as those that are not visible above the level of the application specification.

Life Cycle Phase	*Security Concern*	*Preferred Security Process to be Applied*
I. INITIATION	A. Understand the security problem: identify security risks; determine their magnitude; identify areas where safeguards are needed.	_____ Risk Analysis
	B. Define security requirements.	
II. DEVELOPMENT DEFINITION DESIGN PROGRAMMING TESTING	A. Validate security requirements.	_____ Risk Analysis VV&T
	B. Assess recommended and implemented safeguards; determine whether they satisfy requirements.	_____ Certification
	C. Approve for operation.	_____ Accreditation
III. OPERATION AND MAINTENANCE	A. Reassess security risks.	_____ Risk Analysis Safeguard Eval. EDP Audit
	B. Reassess safeguards.	_____ Recertification*
	C. Approve for continued operation.	_____ Reaccreditation

*If risk analysis, VV&T, certification and accreditation were not performed during development, they might be performed initially during operation. It is far preferable to perform them during development, however.

Figure 1-1. *Life cycle phases and security processes*

The basic problem in using risk analysis to examine controls lies not in risk analysis itself, but in the use of expected loss as an evaluation baseline. As the impact of safeguards on expected losses becomes less clear, expected loss becomes a less meaningful measure of a safeguard's acceptability. What is needed in evaluating controls is a different baseline against which more objective evaluations can be made. The best baseline for this is that provided by the security requirements themselves. That is why a certification evaluation is the technique being recommended.

1.5.2 Validation, Verification, and Testing (VV&T)

VV&T is a process of review, analysis, and testing that should be performed on a system throughout its life cycle but is particularly cost effective when performed during the early life cycle. Validation determines the correctness of the system with respect to its requirements; verification checks the internal consistency and completeness of the system as it evolves and passes through different levels of specification; and testing, either automated or manual, examines system behavior by exercising it on sample data sets. The performance of VV&T provides a powerful quality assurance technique for applications, and when application requirements include security, VV&T becomes an important evaluation technique for security certification. VV&T is usually performed by the people responsible for developing the application; however, for critical applications it may be done by an independent body.

To save on costs, it is important to draw upon evaluation activities in the application life cycle process itself in order not to duplicate such efforts. Applications that are being developed or have been developed with quality assurance in mind will have a VV&T program interleaved in the life cycle process. For example, the validation activity checks the correctness of a system against its security requirements when such requirements are explicitly stated (Phase IIA, fig. 1-1). Evaluation for certification can also draw heavily on other VV&T evidence, when it exists, and thereby reduce evaluation costs considerably (Phase IIB, fig. 1-1). For further information on VV&T see [FIPS101].

1.5.3 Security Safeguard Evaluation

Security safeguard evaluation is an umbrella term being used here for security evaluations performed by people independent of the application in question but internal to the organizational division in which the application resides. A security officer may head such an evaluation. Security evaluations of this type can be the major contributors to evaluation for certification, particularly since it is recommended that the Accreditor or one of the Accreditors (if there is a group performing this function) be a manager responsible for the application. The organizational proximity of the security evaluators and the Accreditor suggested here makes this type evaluation an internal approach to managing the application and may be the most effective arrangement possible.

These evaluation methods usually partition the problem into manageable pieces that correlate with the different skill areas or organizational entities involved in the application. For example, the security checklist used by the Department of Defense [DoD79] partitions the problem into: security management, physical facilities, personnel, hardware, software security, service personnel, files, internal audit controls, time-resource sharing, contingency plan, and use of service bureaus. Within each area, controls are examined and assessed so that an overall picture of the security posture emerges. Examples of different approaches are checklists [AFI79] [DoD79], control matrices [FIT78], and partially quantitative evaluations that assign weights and ratings to the levels of security achieved by the various controls [PMM80]. There are numerous such methods in use but there is no one method suitable for all applications. For further examples and an in-depth discussion of these methods see [NBS83]. Since this group of evaluation methods has comprehensive lists of controls to look for in evaluating the security posture of an application, it can also be used for determining additional security requirements as well (Phase IIIA, fig. 1-1). Just as with risk analysis, these methods can serve the dual purposes of 1) helping determine security requirements and 2) evaluating safeguards.

1.5.4 EDP Audit

EDP audit, a subdiscipline within internal audit, assesses the controls in an organization's system that rely on computers. It determines how well these systems are complying with management's control objectives for these systems and reports its findings to upper management. When control objectives for security (a high-level form of security requirement) are considered, EDP audit becomes a form of security evaluation usable for certification. However, since EDP audit is usually located outside the organizational unit responsible for the application in question, and, since it usually has a broader scope than security, EDP audit would usually be a secondary contributor to a certification evaluation. Since EDP audit methods typically identify a comprehensive set of controls, they can be used for helping determine security requirements as well (Phase IIIA, fig. 1-1). There are numerous EDP audit methods that have been developed by auditing firms and the U.S. General Accounting Office. Some examples are [AAC78], [MAI76], [PMM80], [CIC75], and [GAO81-2,3]. For further discussion of these methods see [NBS83].

1.5.5 Comparison Of Security Safeguard Evaluation And EDP Audit

With respect to the technical processes themselves, security safeguard evaluation and EDP audit have many similarities. For example, both assess compliance with policies; both assess the adequacy of safeguards; both include tests to verify the presence of controls. However, since EDP

audits are generally broader in scope (e.g., part of a general internal review), EDP audits often address issues, such as cost and efficiency in achieving mission objectives, that are outside the purview of evaluations for certifications.

The primary difference between security safeguard evaluation and EDP audit is that safeguard evaluation takes place within the bounds of application responsibility, whereas EDP audit usually takes place outside these bounds. EDP audit is usually not performed under the oversight of an application manager. Furthermore, EDP audit findings for an application are typically reported at a higher level than the person directly responsible for the application. It is an external evaluation procedure used by higher-level managers in managing the agency.

Beyond these differences, there are others of a more subtle nature. For example, EDP audits in general place more emphasis on data reliability [GAO81-3] and validate the data processed by the application (i.e., "substantive" testing). In a security safeguard evaluation, file inconsistencies are of interest mainly to the extent that they reveal inadequacies in the safeguards. As another example, EDP audits tend to be concerned with threats anticipated by application developers and thus tested for in the application and in audit journals. Security safeguard evaluations, while also concerned with anticipated threats, are often additionally concerned that safeguards counter threats in which the application is used in ways not anticipated or intended by its developers. Penetration of an application through a design flaw is an example of an unanticipated threat. Analyses of these two forms of threats require different skills.

As both EDP audit for security and security safeguard evaluation evolve, some differences are lessening and more overlap of concerns is occurring. For example, the historical limitation of EDP audits to financial concerns is diminishing, as is the historical limitation of security safeguard evaluation to violations associated with unauthorized disclosure. EDP audits are being broadened to consider the entire spectrum of computer applications that are being used to manage agency information resources; and security safeguard evaluations increasingly consider exposures such as agency embarrassment or competitive disadvantage that were formerly primarily of concern to auditors. Differences expected to remain, however, are that EDP audit will continue to be broader in scope and will remain a review external to the application whereas security safeguard evaluation will remain a review internal to the application location in the organization.

2. PERFORMING CERTIFICATION AND ACCREDITATION

This section presents guidance on performing certification and accreditation. It applies to certifications performed during either development or operation. Recertification and reaccreditation are also discussed. The section is organized as follows:

2.1 Planning. What preliminary steps are needed before the central part of the evaluation activity can begin? How much evaluation depth is needed?

2.2 Data Collection. How is information gathered for evaluations?

2.3 Basic Evaluation. What is involved in performing a basic security evaluation for certification? What evaluation methods are applicable?

2.4 Detailed Evaluation. What is involved in a detailed evaluation? What methods are applicable to detailed evaluation? How can evaluation analysis be focused?

2.5 Report of Findings. What does the security evaluation report contain?

2.6 Accreditation. What issues are considered in making the accreditation decision? What does the accreditation statement contain?

2.7 Recertification and Reaccreditation. When are recertification and reaccreditation needed? What activities are involved? How are changes controlled?

Figure 2-1 summarizes the certification process. It is an iterative process. That is, based on findings from each stage, previous stages might have to be reentered and work performed over. For example, basic evaluation might identify a function that is not included within evaluation boundaries but that is important for security. This can require revision of the boundaries defined during planning, along with additional data collection.

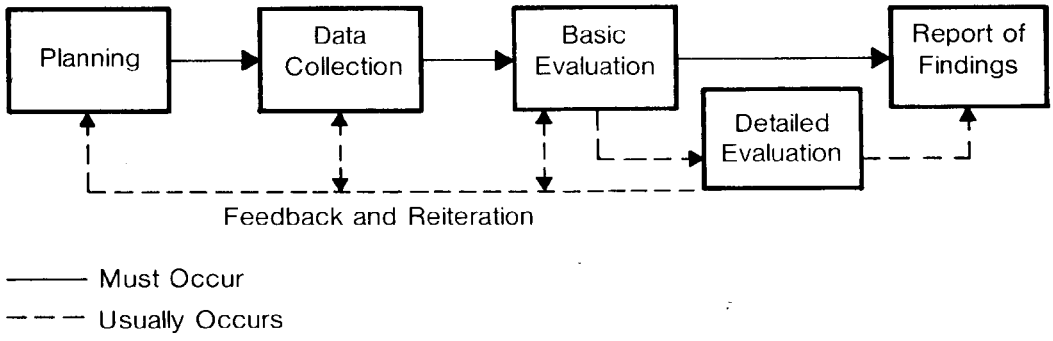

Figure 2-1. *The certification process*

The work is not as sequential as the figure suggests. Typically most or all of the stages are ongoing at the same time. The intent of the figure is to show the shift in emphasis as work progresses.

"Basic" evaluation means "high-level" or "general" evaluation and is the minimum necessary for a certification to take place. In general, basic evaluation suffices for most aspects of an application under review. However, most certifications also require detailed work in problem areas, and therefore require detailed evaluation as well.

Time and resources required to perform a certification vary widely from case to case. In all cases, however, a balance must be kept between potential security risks and certification costs. If possible loss or harm is low, certification costs must also be kept low. Risk analysis can help in deciding how much certification review an application can afford. Typical resources for certification can vary from several person-days to many person-months. Minimum products required from certification and accreditation are a security evaluation report and an accreditation statement.

The certification process described here takes the form of a functional description. It tells what must be done and presents a general functional view of how to accomplish it. It does not present a detailed step-by-step method for performing security evaluation. Detailed specifics of security evaluation differ widely from case to case. Any evaluation method must be adapted to meet situational needs. There is no short cut that avoids the analysis required for this situational adaptation. Detailed methods and aids such as matrices, flowcharts, and checklists are helpful in the adaptation process. This Guideline identifies such aids and methods and shows where they are best applied. However no single detailed method or aid exists that can be used universally. The value of this Guideline is in organizing and focusing the adaptation process. [NBS83] presents summaries and analyses of numerous detailed methods and aids, and is an important complement to this Guideline. [NBS83] also reaffirms an important point that bears repeating, i.e., that the fundamental requirement for successful evaluation is effective, experienced people. No methodology can offset this need.

The certification process presented here is an example. The intent is to provide guidance, not to impose a specific structure. The process is complete and generally applicable to all situations, although the appropriate level of effort varies with each situation.

Since the overall certification process described is at a functional level, it can be applied to both applications under development and those already operational. Functionally, the two situations are similar. For example, both follow the stages of figure 2-1; both include review of similar application documentation such as Functional Requirements Documents and test procedures and reports.

On the other hand, detailed evaluation methods used within the certification process differ for the two situations due to differences in both the types of data available and the organization of the work.

1. *Data Available.* Certifications performed in parallel with development are more apt to have available security-relevant products from the developers. Such products might include vulnerability analyses and security design trade-off analyses. Certifications performed on operational systems have operational documents such as problem reports, audit journal data, availability statistics and violation reports that are not available during development.

   Applications under development might be reviewed for acceptability by several offices or by a Project Steering Committee. These reviews can be used to gather evidence for certification and are discussed further in Appendix F. Operational applications have users who can be interviewed and can provide unique forms of certification evidence based on their personal experience.

2. *Organization of Work.* Certification activity during development is event-driven, being interleaved with the development process and based primarily on the availability of application documentation. Interim certification findings can be used to influence the development process itself. Certification work assignments can thus have peaks and valleys of activity as the development process occurs. Appendix F describes the interleaving of certification with development. Evaluation of an operational application can follow a more circumscribed, project-oriented structure and rely on a skill-based partitioning of the application.

2.1 Planning

The planning process is, in itself, a "mini" basic evaluation[4]. This is so because the plan must anticipate problem areas, needs for specialized skills, needs for support tools, and other issues that cannot be determined without insightful situation-specific analysis. Indeed, the planning process might even determine that further evaluation is not required. This might be the case, for example, if planning analysis revealed general controls to be so weak that further evaluation would be of little value. (In such cases the application still requires a security evaluation report and an accreditation decision.) Planning thus requires expertise in and knowledge of both the application and the certification process. The enlistment of external support might be required to assist in planning.

Some of the planning questions posed below are not answerable at the beginning of the effort. This is especially true of certifications of systems under development, since detailed application characteristics and much documentation are not available early in the development effort. The only approach is to consider as many issues as possible and to continue planning in parallel with evaluation activities. Planning discussion centers around four topics:

1. Initiation (getting started)
2. Analysis (determining what needs to be done)
3. Resource Definition (determining what is needed to do it)
4. Application Certification Plan (documenting the plan)

2.1.1 Initiation

For operational applications, certification and accreditation activities begin at a scheduled time, as determined by appropriate authorities such as the Accrediting Officials or the Certification Program Manager. For applications in the planning stage, certification and accreditation activities begin

4. Two examples of "mini" basic evaluation questionnaires are [IBM80] and [GAO82-2].

early in the Initiation Phase of application development. The certification and accreditation program must assign responsibilities for identifying sensitive applications and for deciding which ones require certification and accreditation.

The individual responsible for managing the certification effort is referred to in this document as the Application Certification Manager. The first step upon initiation of a certification is for the Application Certification Manager to contact both the application sponsor (i.e., office responsible for the application) and the responsible Accrediting Officials. A formal introduction (e.g., via official points of contact and letters of introduction) might be desirable. The cooperation of these three individuals is crucial to the success of the effort. Together they must define the certification effort at a general level. Questions such as the following are answered.

1. What is the application involved; how sensitive is it; where are its major boundaries; where are the major anticipated problem areas; was/is security a major developmental objective; what major technological specialties are relevant?
2. How much money and time are available and appropriate for the certification; does an application risk analysis exist to help in determining appropriate certification costs?
3. Who are the responsible people; what are their roles?
4. Are there major special objectives or concerns that influence the desired quality or level of detail of the certification work?
5. Are there any special restrictions that might constrain the work?
6. Is good documentation available that describes the application and its controls; does prior review evidence exist?

It is presumed that Accrediting Officials are the primary audience for the evaluation products. Additional potential audiences are identified if this might affect the work.

It is important for the Application Certification Manager to document these issues so that a record exists of both the initiation and the initial guidance. A memorandum is suggested for this purpose, with copies sent to the Accrediting Officials and sponsoring office.

2.1.2 **Analysis**

This is the major planning activity. It is performed by the Application Certification Manager with other support as required. Analysis focuses on five major topics:

1. Applicable Policies and Requirements
2. Evidence Needed
3. Bounding and Partitioning
4. Areas of Emphasis
5. Level of Detail

Each topic is discussed below.

2.1.2.1 Applicable Policies And Requirements—Certification is the process of judging compliance with policies and requirements. It is important, therefore, that the Application Certification Manager begin by examining applicable policies and requirements since these, along with the evidential needs discussed below, represent the framework against which security evaluation for certification takes place. Applicable external policies and requirements include laws, regulations, standards, guidelines, and court decisions. Internal policies (e.g., quality assurance, test, development, and auditability standards) are also examined. Some internal policies might be very specific, addressing acceptance criteria, limits on exposures, data sensitivity, or other security-related issues. Finally, security requirements for the application itself are examined.

2.1.2.2 Evidence Needed—Evidential needs for accreditation are important in defining the specific certification evaluation methods and products required. Ideally, the evidence required for agency accreditations is standard throughout the agency and is defined in the overall agency Certification and Accreditation Program Manual (see Sec. 3.1.2). The agency's evidential accreditation requirements must then be translated to the implementation level for each particular effort. Situational variations in evidential requirements can arise for many reasons. For example, past areas of application weakness, violations, or problem reports can necessitate the collection of detailed evidence in narrow areas. Some evidence might already exist that does not need to be duplicated. The Accrediting Officials might have personal preferences for additional types of information. Planning must accommodate these situational needs while at the same time ensuring some level of standardization of certifications and accreditations within the agency.

2.1.2.3 Bounding And Partitioning—In deciding what to do, it is also necessary to decide what not to do. The Application Certification Manager must *establish boundaries* for certification. The general rule of thumb is that the certification boundaries of an application must be drawn to include all relevant facets of an application's environment, including the administrative, physical, and technical areas. Without this, certification gives an incomplete and perhaps misleading picture of application security. For example, technical controls might be excellent but worthless if administrative security is not properly defined (e.g., separation of duties) or if physical security is inadequate.

As an example, the National Aeronautics and Space Administration (NASA)[5] has determined that in most of its sensitive applications users employ the computer center as a service bureau, and control the execution of their own application software programs through remote devices. In these cases, NASA limits certification review to user data entry, application software, and user requirements and specifications for computer center support. The computer hardware, operating system, and data processing activities not under the control of application user management are not considered integral to the application and are thus not included in the application certification review. [For completeness, however, the relevance of the security of computer components outside the application (e.g., hardware, operating system) must be discussed in the evaluation report.] On the other hand, for stand-alone applications that employ a dedicated computer, NASA certification reviews include the hardware, operating system, and associated data processing activities.

As boundaries are formulated, it is important to explicitly record security assumptions that are made about areas outside the boundaries. For example, if the operating system is excluded from certification review, it should be explicitly recorded that the operating system is assumed to provide a sufficiently secure base with respect to such things as process isolation, authentication, authorization, monitoring, maintaining the integrity of security labels, and enforcing security decisions. These assumptions are made known to the Accrediting Official(s) via the security evaluation report.

Once boundaries have been established, the Application Certification Manager must decide how to *partition the work* within the boundaries. Sometimes one person has the skills and experience to perform the full evaluation. More often a team is required, due to the range of experience needed. Figure 2-2 shows a sample partitioning; most certifications do not require evaluation in all of the areas shown.

External reviews often suffice in some of these areas. For example, reviews of physical and personnel security might have been done for the organization as a whole. An internal control review for compliance with [OMB81] might exist for administrative and accounting controls. The operating system and hardware might have already been evaluated by the DoD Computer Security Center, which provides product evaluations and an Evaluated Product Listing for computer security [DoD83].

When the certification is being performed in parallel with development, different skills are applicable to the different developmental phases. Appendix F shows which skills apply in which phases.

In partitioning the work, the Application Certification Manager examines several characteristics of the application in order to estimate required numbers and skill levels of security evaluators,

5. NASA has developed a certification program [NASA82] in parallel with the development of this Guideline.