Admin. Security	Computer Operation	Contingency Planning	Change Control	Data Entry and Output	Operating System	Communication Security
Personnel Security	Physical Security	Environmental Controls	Development Method	Application Software Controls	Data Base Management System	Hardware

Figure 2-2. *Sample partitioning of security evaluation responsibility areas for a sensitive application*

required evaluation time, and required evaluation activities. The major characteristics examined include application size, complexity, and documentation quality.

- *Size* is a critical planning factor. The larger the application or partition, the greater the required time and number of people.

- *Complexity* is based on factors such as the nature of the functions being performed, the extent to which operating system specifics need to be examined, and the clarity and level of abstraction of the languages used (whether procedural or programming). Size and complexity are assessed not just for the application as a whole, but also for each of its component parts.

- *Documentation quality* is an important consideration in planning the evaluation. There are a number of questions to ask here. Does an application flow diagram exist? Is a listing of controls available or will this information have to be gathered from application documentation? Does documentation distinguish security controls from other functions? Do functional requirements documents, system specifications, test documentation, procedure manuals, and other documents exist? Are they up to date? Are they accurate and complete? Are they understandable? Especially for requirements documents, do people agree with them?

There might be other characteristics of the application that can affect the evaluation. Examples are a distribution of functions over physically separate sites and anticipated resistance from application personnel.

2.1.2.4 Areas Of Emphasis—An evaluation must encompass the entire application, not just its major security components, since it cannot be assumed that security-relevant areas are correctly identified. The reason for this comprehensiveness is that security deficiencies can occur almost anywhere, and sometimes arise in very unlikely places. This must be balanced against the facts that (1) evaluation resources are usually very limited, and (2) some areas (e.g., functions applicable only to nonsensitive assets) warrant less detailed coverage than others (e.g., password management). What is needed is a plan that achieves the proper blend of completeness and focused emphasis.

In general, the greatest emphasis is placed on those assets, exposures, threats, and controls associated with areas of greatest expected loss or harm. Other factors are also influential. For example, less emphasis is placed on areas where flaws are believed to be well known and understood. (Nevertheless, the existence of these flaws is addressed in the evaluation findings.)

There are many factors, in addition to the Application Certification Manager's basic experience, that can influence the proper placement of emphasis. Problem areas might have been identified by prior certifications. Audit or evaluation findings, risk analysis findings, and violation reports might identify areas of weakness and help set priorities. Application personnel themselves might point out weak areas. One method [PMM80] [NBS83] uses a group of application personnel interacting via the Delphi method to identify key areas for evaluation emphasis.

2.1.2.5 Level Of Detail—Probably the single most difficult question in performing an evaluation is: How much is enough? As difficult as it may seem to answer this question generically, there is in fact a useful answer.

- For most areas of an application, a ''basic'' (i.e., high-level overview-type) evaluation is sufficient for an evaluation judgment. Since a ''basic'' evaluation is complete at the functional level, it is also the minimum necessary if cost is a limiting factor.

- Some situations warrant ''detailed'' evaluations, because of their high sensitivity or because their fundamental security safeguards are embedded deep within the computer, out of view of a high-level look.

There are a number of criteria to be taken into consideration in determining the amount of detail needed in an evaluation. In most cases the major criteria are application sensitivity, evaluation evidence, and control location. These are discussed below. Other criteria can also be influential. Examples include (1) the amount of evidential detail needed for Accrediting Official confidence, (2) application size and complexity, and (3) the amount of Application Certification Manager and security evaluator experience, since inexperienced people might require increased detail to gain acceptable confidence in the evidence they are gathering. The decision based on these criteria can apply to the application as a whole or to components within the application.

1. *Application Sensitivity.* In general, the greater the sensitivity of an application or application component, the greater the desirable evaluation detail. Major expected loss areas of highly sensitive applications almost certainly require detailed evaluation. Similarly, basic evaluations should suffice for minor expected loss areas of applications that are sensitive but not critically so. Between these extremes there is much need for judgment.

2. *Nature of Evaluation Evidence.* This is a broad criterion. It includes prior evaluation findings, prior violation/problem reports (for operational reviews), and new evidence obtained during the evaluation (for both operational and developmental reviews). The former two indicate areas of past strength and weakness, suggesting the need for less or more evaluation detail. The latter area, evidence obtained during the evaluation, might be the single most important criterion, and also results in decisions for more or less detail. For example, the planning portion of an evaluation, via its ''mini'' basic evaluation (see Section 2.1), might determine that the application has never addressed security and is in a completely insecure state. In this case, the planning process itself might suffice for an evaluation with a basic evaluation perhaps performed later, once the major problem areas have been resolved. A detailed evaluation is inappropriate in the face of gross or fundamental security inadequacies. A detailed evaluation might also be inappropriate if the planning process reveals application security safeguards to be highly effective and well managed. Judgment is needed here, but the objective is to minimize the expenditure of certification resources on applications having either highly effective or highly ineffective security safeguards. It is usually preferable to place more certification attention on intermediate cases.

   As another example, detection of a potential problem area can necessitate more detailed analysis. This might be the case if examination of the software development method finds it provided inadequate procedures for preventing and detecting errors. Even though the application security functions that were implemented seem acceptable, this finding raises the need for more detailed evaluation to provide confidence that the entire implementation can be relied upon.

3. *Control Location.* The issue here is the extent to which application security safeguards are located within the computer, as opposed to the physical and administrative environment that surrounds the computer. Several factors influencing this include the extent to which

   a. the application relies on programmed versus user control.

b. transactions are initiated externally or internally.

c. transaction records are kept externally or internally.

Auditors will recognize these factors as influences on whether an audit is performed "around" or "through" the computer [MAI76, p. 77].

Applications in which control is external are typically evaluated at the basic level. Examples include externally-controlled (1) accounts-receivable or inventory applications, (2) message processing applications, and (3) automated teller applications. Applications in which control is primarily internal require a detailed evaluation. Examples include (1) fully automated funds-disbursement and accounting applications and (2) real-time control applications (e.g., air traffic control, NASA mission, automated production).

2.1.3 **Resource Definition**

Based on the above analysis of what needs to be done in the evaluation, the Application Certification Manager plans the resources needed to accomplish the task (i.e., time, people, administrative support, and technical tools). Time estimates include not only the time required to perform the tasks, but also the time required to acquire the resources.

General administrative support needs and technical tools (discussed in Section 3.3.3) should be defined in the overall agency Certification and Accreditation Program Manual. Other related forms of general support might include copies of documents (e.g., policies, checklists), training, personnel clearances, scheduling of travel.

Typically the most difficult resource to obtain is the people. Section 1.3 discusses required skills and experience and Section 3.3.1 summarizes several staffing difficulties. Required people might include, in addition to security evaluators, consultants, technical writers, and couriers.

For all resource estimates, underlying assumptions should be listed. The assumptions consider contingencies that might affect the availability of people or other resources.

2.1.4 **Application Certification Plan**

Based on the analysis and resource definition that has taken place, it is important to now draw up and document a plan for certifying the application (the Application Certification Plan). This plan is typically issued by the Application Certification Manager and is coordinated with involved parties before its issuance. Accrediting Official approval can also be useful, depending on the extent of any support required from the Accreditor's organization, but this support should be kept to a minimum. Production of a large document should be avoided, since evaluation resources typically cannot afford this. The agency Certification and Accreditation Program Manual can be heavily referenced and generally suffices for much of the Application Certification Plan. The Plan should be followed closely unless and until unforeseen problems arise that indicate a need to revise or modify the Plan. The Plan should include scheduled opportunities for such revisions or modifications. With more experience in planning certifications and accreditations, these revisions may become less frequent.

2.1.4.1 Contents Of The Plan—Figure 2-3 shows a sample outline of the Plan. Each section of the outline is briefly described below.

1. *Executive Summary.* This is addressed to the Accrediting Officials, and includes all they need to know about the effort.

2. *Introduction.* This identifies the application (and its major boundaries), the sensitivities involved, the Accrediting Official(s), special objectives or restrictions, general schedule constraints, and other situation-specific information such as sources for specific security

1. EXECUTIVE SUMMARY

2. INTRODUCTION
   2.1 Application Background
   2.2 Scope of Certification

3. RESPONSIBILITIES
   3.1 Evaluation Team
   3.2 Other Offices

4. EVALUATION
   4.1 Security Requirements
      4.1.1 Laws, Policy, User Needs
      4.1.2 Documentation

   4.2 Evaluation Approach
      4.2.1 Basic Evaluation Tasks
      4.2.2 Detailed Evaluation Tasks

5. SCHEDULE

6. SUPPORT REQUIRED
   6.1 Administrative
   6.2 Technical

7. EVALUATION PRODUCTS

APPENDICES
A. Accreditation Statement(s)
B. Tools to support technical evaluation (e.g., checklists)

Figure 2-3. *Sample outline for an application certification plan*

policies and requirements applicable to the application, or existing security requirements documents.

3. *Responsibilities.* Organization structure and responsibilities are identified for both the evaluation team and other offices. The partitioning of evaluation work is defined. Of particular note are any specific responsibilities of application line personnel in support of the effort. The relationship of the evaluation team to other agency offices is defined.

4. *Evaluation*

   a. *Security Requirements.* This section describes the tasks necessary for obtaining a satisfactory listing of the application's security requirements. If a security requirements document was written when the application was developed, this task is simple. If no such document exists, the evaluators will need to interview users and review applicable regulations, laws, and agency policy. A risk analysis may prove helpful for this purpose.

   b. *Evaluation Approach.* This section enumerates the tasks needed to accomplish the basic evaluation and any detailed evaluation deemed necessary. The partitioning of the evaluation work is defined. The specific tasks will probably differ for different partitions of the evaluation and might also differ between operational and developmental situations, as discussed in Sec. 2.1.4.2. General topics addressed should include: (1) the areas of emphasis, (2) levels of detail, (3) specific evaluation tasks and techniques, (4) people to be interviewed, and (5) documents to be reviewed.

5. *Schedule.* The schedule includes milestones, products, assumptions, and required inputs (e.g., briefings, documentation). The timing of the milestones is based on the time estimates articulated during resource definition (see Section 2.1.3).

6. *Support Required.* Both administrative and technical (i.e., hardware/software) support requirements are listed, as is any support required from other agency offices and application line personnel.

7. *Evaluation Products.* The security evaluation report is the primary product. This section identifies any variance from the defined report and evidence found in the overall agency Certification and Accreditation Program Manual.

8. *Appendices.* A sample accreditation statement is included. It is important that the Accrediting Officials have a clear understanding, before the effort begins, of what the statement might contain so that the contents of the security evaluation report do not come as a surprise. Also included or referenced is information on methods and tools to be used during the evaluation.

2.1.4.2 Illustrative Task Structure For Evaluation—An illustrative high-level task structure is shown below. Differences between developmental and operational certifications will show up in the details of carrying out these tasks. For example, under security testing, a developmental certification will use test data only, but an operational certification will also have available journals and logs.

1. Indoctrination—briefings, tutorial overviews.

2. Security Requirements Review—list documents to be reviewed and commented upon and interviews to be performed.

3. Security Design/Operation Review—list design documents (for developmental and operational systems) and performance documents (for operational systems) to be reviewed, commented upon, and analyzed.

4. Security Testing—list documents to be reviewed and commented upon, any operational testing to be monitored, and security testing to be defined and performed.

5. Security Support—list potential tradeoff studies, detailed analysis, and other ad hoc analysis and support.

6. Report of Findings.

2.1.4.3 Initiating The Evaluation—The first step in initiating evaluation proper involves obtaining and organizing resources described in the Plan. That is, people are recruited or assigned, resources obtained, an administrative structure established, evaluation methods and tools selected, and assignments made. The central part of the evaluation work then begins.

2.2 Data Collection

Most of the work performed during an evaluation (including the planning phase) serves the purpose of data collection. Often the techniques used to collect data represent building blocks in the construction of evaluation methods. The exact nature of the data to be collected depends on the evaluation methods and tools selected. This section discusses three data collection techniques frequently used:

1. Provision by Application Management

2. Document Review

3. Interviews

Especially for the more general information required in basic evaluation, provision by application management is recommended as the best data collection technique. The reasons for this are discussed below, followed by a discussion of each technique in more detail.

In performing an evaluation, the greatest expenditure of resources occurs not in forming the judgment but in learning the characteristics of the application. There are two major aspects of learning about the application: (1) learning what it does and how it works; and (2) determining its security posture (i.e., threats, assets, exposures, controls). Both of these learning objectives can be met by document review and interviews, as discussed below. From the agency's point of view, however, document reviews and interviews can be very time consuming and consequently less cost effective data collection mechanisms.

Ideally, documentation is the best source for information about the application. Unfortunately much application documentation is of poor quality and in many cases does not exist. On the other hand, where it does exist there can be hundreds or thousands of pages of documentation associated with an application. This documentation might be vague or outdated, and often does not segregate or even explicitly identify security controls. As a learning vehicle, actual application documentation often leaves much to be desired.

Interviews also have major shortcomings. The primary one is that they often are time consuming for the amounts of information produced. A typical interview involves at least a person-day of work, including preparation and documentation time, along with the time of two interviewers and one interviewee. Frequently this cannot be justified for the amount of information obtained in a typical interview for security evaluation purposes.

The basic problem giving rise to this inefficiency is that with document reviews and interviews, the wrong people are gathering the information. The people able to gather information about an application most efficiently are those people most familiar with it, such as developers and users. The least time consuming data collection technique, then, is for application management to provide application information by tasking application developers and users to formulate and present it to the evaluation team.

Where security expertise is required, as in the preparation of security requirements, it is often best for application and certification personnel to work together. For developmental applications, the security evaluators should participate in the requirements review procedures. For operational applications which do not have explicitly expressed security requirements, application and certification personnel should work together to arrive at an accurate understanding and description of these requirements.

It is possible that the data collection process will detect evidence of fraud or crimes. Such evidence must be turned over to appropriate authorities (e.g., the OIG). Care must be taken to consult with the organization's legal staff so as not to take any inappropriate action that might, for example, impede investigation or prosecution or open oneself to legal action.

2.2.1 **Provision By Application Management**

As noted above, there are two major areas for data collection:

1. What does the application do and how does it work?
2. What is its security posture with respect to threats, assets, exposures, and controls?

Application management provision of this information involves the use of application personnel to provide introductory and detailed briefings and tutorials on the application and its security safeguards. It also includes the provision of *four key documents*. Ideally, these documents already exist. Typically, however, most do not and must be formulated for the certification.

- *Security Requirements*—First and foremost are the application security requirements themselves. As discussed below in Section 2.3.1, security requirements are the fundamental baseline for certification and accreditation. If an acceptable statement of requirements does not exist, it must be formulated during the certification. This is best done through a joint effort of certification and application personnel. Certification personnel are needed because typically application personnel do not have a thorough understanding of computer security, especially with respect to external policies. Application personnel are needed because certification personnel usually do not have a thorough understanding of the application, especially with respect to situational user needs and preferences.

- *Risk Analysis*—The second key document is an application risk analysis showing threats and assets [FIPS31 and FIPS65]. This is useful in validating the requirements and in defining the underlying problem to be solved. Again, where this does not exist, it is best prepared through a joint effort by certification and application personnel.

- *Application Flow Diagram*—Third is an application flow diagram showing inputs, processing steps, and outputs. Complete transaction flows must be included for important transaction types. This is critical for an understanding of the application. It is best prepared by application personnel.

- *List of Application Controls*—The final key document is a listing of application controls. Controls can be the most difficult application-specific portion of the security picture for an outsider to define, since they are so varied and situation-specific. On the other hand, this definition is not easy for insiders, either. For example, as application personnel gather this information, one common difficulty they face is the seemingly simple task of distinguishing controls (e.g., authorization mechanisms, sequence checking) from application activities subject to control (e.g., initiation, recording, transcription, calculation). A useful rule of thumb is that a control is any protective action, device, procedure, technique, or other measure that reduces exposure(s) [MAI76, p. 34].

Provision of this information by application personnel can have benefits beyond that of easing the burden of data collection. In particular, it can significantly increase the security awareness of application personnel. This increased awareness alone is a significant benefit. It can also draw the attention of certification personnel to application areas that are not well understood and that might thus warrant closer analysis.

Evaluation personnel should not accept documentation provided by application management as absolutely accurate, since application personnel might not be objective (see both the introduction to Section 1 and Section 3.2). Document reviews and interviews are useful in validating this information. Nevertheless, documentation provided by application personnel often proves to be an excellent source of information, and it has the added advantage of making the certification process as a whole less expensive for the agency.

2.2.2 Document Review

The second data collection technique discussed here is document review. Document review becomes increasingly important as evaluation attention focuses on more detailed issues.

The potential set of documents to be reviewed varies substantially in each certification, depending on evaluatior ›bjectives and the availability and value of documentation. Appendix D presents an illustrative listing of documents that might be reviewed in a very large-scale certification effort. In general, the more detailed the document, the more reviews should concentrate on only security-relevant or sample portions of it. An example of this latter situation occurs when only sample source listings are examined to judge compliance with programming standards.

Some of the documents listed in Appendix D such as violation reports, audit journals, and operational statistics are only available in operational applications. Most are subject to review whether the application is operational or under development.

Appendix D illustrates the differing purposes that can underlie a review. It defines two types of review: critical and research/reference. Critical reviews involve an analysis for security deficiencies. Research/reference reviews help evaluators to understand application functionality and characteristics or reported shortcomings in order to better perform critical reviews. These different purposes might require separate passes through the documents. If evaluation support is being obtained externally, possible deliverable items might include written comments on documents reviewed.

2.2.3 Interviews

Interviews, though time consuming, can sometimes produce information not available through other means. Some guidance already exists on the planning and conduct of interviews as well as on interviewing strategies (since the way in which a question is asked can be as important as the question itself). Appendix E contains an interview procedure developed in support of the U. S. Department of Agriculture (USDA) certification program. Two points about interviews are discussed here: planning the interview and ensuring accurate information.

1. *Planning the Interview.* This must be stressed. Questions such as the following must be answered carefully.

   a. Which people should be interviewed (e.g., managers, users, developers, people from outside the agency)?

   b. What is the subject and purpose of each interview; what expertise is required of the interviewer?

   c. When, where, and under what conditions (e.g., people in attendance) do the interviews take place?

   d. What preparatory activities and materials (e.g., questionnaires, cameras) are needed?

   e. What documentation of the interview is required?

   f. What coordination is needed to arrange the interviews?

   g. Which interviews are dependent on findings from others?

   Questions to be asked during the interview should be prioritized so that important ones are answered early. Questionnaires presented to the interviewee in advance or used during the interview can be useful. At the beginning of the interview, the interviewee should be asked whether a tape recorder may be used. Tape recorders are generally not used since they can dissuade people from discussing sensitive subjects, but occasionally people prefer the recorder because of fear of misquotes. If recorders are used, notes must still be taken since people do not always speak into the microphone properly.

2. *Ensuring Accurate Information.* One purpose of a certification and accreditation program is to provide checks and balances. This purpose is not served if evaluators simply report the opinions of developers and users. Some interviewees may not know the facts and others may knowingly misrepresent them. Also, evaluators may misinterpret the answers. The issue here is information quality. The use of interviews itself, as opposed to simply requiring subjects to complete questionnaires, improves information quality since the personal interaction involved helps in interpreting meanings behind words, counteracting bias, and following leads. Beyond this, there are a number of specific interview techniques in addition to the guidance included in Appendix E that can help to improve the quality of information gathered for certification.

a. Assess subject competence and bias. The subject might not be qualified to discuss certain topics. The subject might also have opinions or vested interests that bias his/her responses.

b. Independently verify and document important facts.

c. Repeat answers to important questions so mutual understanding is ensured. Record key facts immediately, rather than entrusting them to memory. Two interviewers are needed to help ensure accuracy and reduce misinterpretations of answers.

d. Determine facts upon which subject opinions are based. The interviewer might form different conclusions.

e. Tell subjects what will be done with the information. They might as a result be more open.

f. Allow subjects to remain anonymous. They might provide more information as a result.

g. Do not place great reliance on the confidence subjects associate with their own estimates.

h. If the subject's judgment appears faulty (e.g., on threat likelihood or impact), request the subject to construct most-likely, extreme, most-costly, or other scenarios. This can change and improve the subject's opinion. The interviewer should have at hand as many examples of realistic scenarios as possible to counter subject bias, since subjects sometimes form judgments based on the ease with which they can fabricate plausible scenarios. Suggest ranges, whether quantitative (e.g., 0-10, 11-50, over 50) or linguistic (e.g., low, medium, high), to prevent the subject having to formulate precise numbers (e.g., for threat frequency, losses, error rates).

i. Return draft write-up to subjects so that they can (1) correct any errors or misinterpretations by the evaluators or (2) change anything they have said and subsequently learned to be in error.

2.3 Basic Evaluation

As described in this Guideline, the security evaluation process has two levels of detail: basic evaluation and detailed evaluation. This section discusses the former; Section 2.4 the latter. As noted in the introduction to Section 2, basic evaluation typically suffices for most aspects of an application under review, although most applications also require some detailed evaluation work in problem areas. Section 2.1.2.5 presents some criteria for helping to determine when detailed evaluation is warranted.

The general distinction between basic and detailed evaluation is that basic evaluation is primarily concerned with the overall functional security posture, not with the specific quality of individual controls. For example, basic evaluation is concerned with whether access authorization at the file level is sufficient or whether it might be required at, say, the record level. As another example, it might be concerned with whether authorization subjects must include terminals or just, say, individuals and processes. Basic evaluation is also concerned with verifying that security functions actually exist and that the implementation method is of sufficient quality to be relied upon. Detailed evaluation, on the other hand, is concerned with whether security functions work properly, satisfy performance criteria, and acceptably resist penetration.

There are four tasks in a basic evaluation:

1. security requirements evaluation (are application security requirements acceptable?)

2. security function evaluation (do application security functions satisfy the requirements?)
3. control existence determination (do the security functions exist?)
4. methodology review (does the implementation method provide assurance that security functions are acceptably implemented?)

Each task is discussed below. As noted in the introduction to Section 2, basic and detailed evaluations can be performed during application development or after an application has been in operation for a period of time. Appendix H presents a simple example of activities that might be involved in a basic evaluation using the above task organization.

2.3.1 Security Requirements Evaluation

The major purpose of certification is to determine whether application safeguards satisfy security requirements. This process is only meaningful if the application has well-defined security requirements. Unfortunately, most applications do not. For certification to be useful, then, the security requirements imbedded in the application must be critically examined to determine whether they are reasonable and whether they comply with federal, agency, and user requirements. The requirements in question are typically those embodied in the Project Request [FIPS64], where such a document exists. Where these requirements are not documented, they must be formulated.[6] Accurate, complete, and understandable security requirements are fundamental to certification.

In both formulating and evaluating security requirements for an application, two classes of needs are considered: policy needs and situational needs. Policy needs derive from the principles and required practices that the application is obligated to pursue, such as Federal laws, regulations, standards, and agency policies. Situational needs are those deriving from the application's characteristics and environment. To determine situational needs, four primary areas are considered: assets, threats, exposures, and controls.

1. *Assets.* What should be protected?
2. *Threats.* What are assets being protected against?
3. *Exposures.* What might happen to assets if a threat is realized?
4. *Controls.* How effective are security safeguards in reducing exposures?

These are discussed further in Section 2.4.2.1. If a risk analysis has been performed for the application or its environment, many situational security needs might already be well defined.

There is a rapidly growing body of useful guidance becoming available to assist in requirements definition and evaluation. The most directly applicable (in lieu of a detailed agency security policy) are those computer security policies, standards, and guidelines now being issued by the Federal government, such as the internal control standards mandated in [OMB81] and the NBS guidelines, standards, and other NBS publications that complement this one. For example, [FIPS73] includes a discussion of application controls. Requirements formulated in other agencies can also be useful (see Appendix B for references). One promising approach to defining requirements is use of the set of evaluation criteria formulated by the DoD Computer Security Center [DoD83]. These criteria represent a categorization of security levels for computer systems based on security functions and system quality. Still other useful tools are computer security checklists and questionnaires (e.g., [AFI79, CIC75, EAF83, FAIM, FIT78, FIT81, GAO81-2, HHS78, IBM83]). Several of these are summarized in [NBS83]. Risk analysis methods (e.g., [FIPS31, FIPS65, SDC79]) are useful

[6] In the EDP audit field, control objectives express overall application requirements. When control objectives address security, the control objectives become security requirements.