FBI Electronic Recordkeeping Certification Manual

Prepared for:

Department of Justice
Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

April 30, 2004

Under Contract GS-23F-97806F
Document Control Number: 1970061—ERKM—Final V1.0

Prepared by:

SRA International, Inc.
2000 15th Street North
Arlington, VA 22201

For Official Use Only

Executive Summary

The mission of the Federal Bureau of Investigation (FBI) is to uphold the law through the investigation of violations of federal criminal law; to protect the United States from foreign intelligence and terrorist activities; and to provide leadership and law enforcement assistance to federal, state, local and international agencies. Vital to the support of the FBI mission is the implementation of records management policies and procedures that ensure the proper creation, maintenance, use and disposition of records.

The FBI, like all other Federal agencies, is required by statute to "make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency."[1] This practice of ensuring "adequate and proper documentation"[2] is essential to efficient and economical agency operations by guaranteeing that information is documented in official files, including electronic recordkeeping (ERK) systems, where it will be accessible to all authorized staff that may need it.

As the FBI evolves from paper-intensive records and information management systems to more electronic, paperless records and information management systems, electronic information systems (IS) containing records must comply with the policies and procedures governing the management of FBI records.

The Assistant Director of the Records Management Division (RMD) is the FBI Records Officer (RO). On April 29, 2002, the Director of the FBI delegated to the Records Officer the authority to determine what FBI information constitutes a record under Federal Law and the authority to approve, or withhold approval of, any electronic information or knowledge management (KM) system in use or under production.[3] No electronic information or knowledge management system is to be utilized in the conduct of FBI business without the approval of the FBI RO.

The RO's highest priority is to ensure that support for records management criteria is incorporated into requirements specifications and test plans of new information and knowledge management systems. The second highest priority is to review existing systems within the FBI to ensure compliance. Development efforts may continue on new information systems; however, it is incumbent on the Project Manager of any information or knowledge management system in development to ensure coordination with the Records Officer, as the system may not become operational absent RO authorization. To this end, the FBI created the Electronic Recordkeeping Certification (ERKC) process as described in this manual.

Implementation of the ERKC process ensures that the systems the FBI develops and maintains comply with statutory and agency electronic recordkeeping requirements. The ERKC process incorporates electronic recordkeeping requirements into the system development life cycle

[1] Federal Records Act, Title 44 U.S.C § 3101 (1950)
[2] Phrase was originally used in the Federal Records Act of 1950 that established records management as a basic responsibility of all Federal agencies.
[3] *Records Management Division Delegation of Authority to the Agency Records Officer*, Electronic Communication (EC), Case ID # 66F-HQ-A1358157; April 29, 2002.

(SDLC) so that all system development activities can appropriately consider electronic recordkeeping issues from the earliest stages of acquisition and design.

The ERKC is a process used to evaluate system compliance with records management criteria. The process is designed to guide system sponsors and developers in assessing and incorporating records management criteria into system requirements specifications, and then ensuring fulfillment through review of documented test results. The ERKC process consists of identifying systems that contain records, helping System Owners and developers understand ERK criteria, ensuring that system requirements specifications satisfy ERK criteria, and validating ERK functionality through review of system test results.

Forming partnerships with other information professionals is essential. The ERKC process is designed to leverage the outputs from existing IT systems management processes to minimize redundant data capture and reduce the burden on systems development and management activities.

❖ ❖ ❖

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

❖ ❖ ❖

RECORD of CHANGES

Version/Change	Date	Description	Entered By

Foreword

This Electronic Recordkeeping Certification (ERKC) manual presents the processes for obtaining electronic recordkeeping (ERK) certification from the perspective of FBI headquarters organizations. However, it frames a relatively generic process that regional and field organizations can tailor to meet their specific needs based on the principles and processes outlined herein.

As several related FBI information technology management processes [e.g., system development life cycle (SDLC) and capital planning and investment control (CPIC)] continue to evolve, this manual may similarly change over time to remain consistent with these other processes. Readers should ensure that they are using the most current version of this manual. The FBI Records Management Division (RMD) will post the most current version of this manual on the RMD page of the FBI intranet.

❖ ❖ ❖

Section One—Introduction

This section provides an introduction to the Federal Bureau of Investigation's (FBI's) electronic recordkeeping certification (ERKC) process. It describes the objectives of the ERKC manual, the context of the process within the FBI's broader recordkeeping program, and the goals of the process. It also introduces some fundamental terminology used in the ERKC process. A description of the section contents of this document is provided in Table 1-1.

Table 1-1. Document Section Contents Summary

Sec. No.	Sections/Subsection	Description
1	Introduction	This section provides an introduction to the Federal Bureau of Investigation's (FBI's) electronic recordkeeping certification (ERKC) process. It describes the objectives of the ERKC manual, the context of the process within the FBI's broader recordkeeping program, and the goals of the process. It also introduces some fundamental terminology used in the ERKC process.
2	ERKC Process	This section describes the ERKC process and relates it to the FBI's capital planning and investment control (CPIC), system development life cycle (SDLC) and security certification and accreditation (C&A) processes. It also describes the differences in the ERKC process for new and legacy systems.
3	Roles and Responsibilities	This section defines the roles and responsibilities of FBI System Owners and the Records Officer (RO) within the ERKC process.
Appendix A	References	This section provides documents references.
Appendix B	Glossary	This section provides a glossary of terms used in this document.
Appendix C	ERK Assessment Criteria	This section presents the ERK Assessment Criteria.
Appendix D	ERKC Process Flow for New Systems	This section presents the ERKC process-flow model for new systems.
Appendix E	ERKC Process Flow for Legacy Systems	This section presents the ERKC process-flow model for legacy systems.
Appendix F	Risk Management	This section provides detailed guidance on performing risk management in the context of determining vulnerabilities associated with the processing and use of electronic records.
Appendix G	System Evaluation Process Details	This section provides detailed guidance on performing ERK certification evaluations.
Appendix H	ERK Criteria Tailoring Tool	This section presents the ERK Criteria Tailoring Tool, which assists in determining the criteria that are applicable to the system under consideration.
Appendix I	ERK Compliance Evaluation Worksheet	This section presents the ERK Compliance Evaluation Worksheet.
Appendix J	ERK System Certification Report Template	This section provides a template for the ERK System Certification Report, which should contain the Worksheet as an appendix.
Appendix K	ERK Certification Letter Template	This section provides a sample ERKC Letter template.
Appendix L	ERKC Electronic Communication Template	This section provides an ERKC electronic communication (EC) template.
Appendix M	FBI RMA Metadata List	This section lists the metadata elements required for all FBI ERK systems.

1.1 Objectives of the Manual

The FBI's ERKC manual accomplishes the following objectives:

- Defines the authorities, roles, responsibilities, processes, and documentation requirements that govern the certification of FBI-owned and FBI-sponsored information technology (IT) systems.
- Serves as a guide for system developers, system owners, project managers, and certification team members to the activities required for an FBI-owned or -sponsored information system (IS) to achieve Bureau electronic recordkeeping certification.

1.2 The FBI Electronic Records Management Program

The FBI is required under Federal statute (44 U.S.C. 31) to establish a records management program, defined as a planned, coordinated set of policies, procedures, and activities needed to manage an agency's recorded information. Chapter 36 of the Code of Federal Regulations (36 CFR 1222.20) and OMB Circular A-130, *Management of Federal Information Resources*, require that agencies integrate records management into their overall information resources management (IRM) program.

1.3 Goal of Electronic Recordkeeping Certification Process

The goal of the ERKC process is to ensure that electronic recordkeeping compliance requirements, including the proper creation, maintenance, use and disposition of Bureau records, are incorporated into the design and deployment of new information and knowledge management systems [hereafter collectively referred to as information systems (IS)] and that all existing FBI systems are also in compliance. Compliance requires that certain criteria are satisfied. These criteria are evaluated during the ERKC process.

1.4 Electronic Recordkeeping Certification (ERKC)

The Electronic Recordkeeping Certification (ERKC) process described in this manual is the FBI's official process to comprehensively evaluate the technical and non-technical electronic records management features of FBI information systems and to determine whether they satisfy the ERK compliance criteria. The certification determination can take one of the following forms:

- *Approval to Operate (ATO)*—approval to operate a system because it meets all recordkeeping criteria (ATOs must be recertified every three years),
- *Interim Approval to Operate (IATO)*—temporary approval to operate a system for a defined period of time and under certain defined conditions, or
- *No Approval to Operate (NATO)*—denial of approval to operate a system because it fails to meet recordkeeping criteria.

In addition, the ERKC process provides standardized methods of evaluating a system for ERK compliance and recognizes four architectural approaches to achieving such compliance:

- *Integration*—an approach based on integrating a Department of Defense (DoD) 5015.2-certified Records Management Application (RMA) with the information system for which certification is sought.
- *Direct Export*—an approach based on incorporating the necessary features within the information system for which certification is sought such that the system is able to automatically export Federal records and their associated metadata to an existing shared FBI RMA. (*Virtual Case File* will include an RMA in its architecture, so exporting records to it is a recognized option.)
- *Integral*—an approach based on designing and building an information system such that it performs all of the necessary ERK functions internal to the system itself.
- *Deferred*—an approach intended to permit temporary certification for information systems that are designed and built for specific purposes in response to tactical or emergency situations (e.g., response to the D.C. sniper investigations). Once the emergency situation is over, owners of such systems must determine whether to (1) dispose of the system and transfer all appropriate records to an approved RMA or (2) request certification for the system if it will have recurring use in the future.

1.5 Availability and Comments

Copies of this manual may be obtained from the FBI's Records Management Division (RMD) as well as from the RMD page on the FBI intranet. All comments concerning this document and its content should be addressed to the following office for action.

Chief, Records Automation Section
Records Management Division
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, D. C. 20535-0001

Please ensure your return name, phone number, and email address are included for a direct response.

Section Two—Electronic Recordkeeping Certification (ERKC) Process

This section describes the FBI's electronic recordkeeping certification (ERKC) process. It presents approaches for both new and legacy systems. While ERK criteria are the same for both new and legacy systems, the processes for obtaining certification are different. Section 2.1 illustrates the relationships among the FBI's electronic recordkeeping certification, capital planning and investment control (CPIC), system development life cycle (SDLC), and security certification and accreditation (C&A) processes. It then summarizes the four principal phases of the ERKC process: Definition, Verification, Validation, and Post Certification. Section 2.2 describes the ERKC process for new systems. Section 2.3 describes the ERKC process for legacy systems.

2.1 Overview of the ERKC Process

The FBI's ERKC process—which is contingent upon a finding by the Records Officer (RO) that a system has records under Federal law—is complementary to and logically linked with the FBI's CPIC, SDLC, and C&A processes. Figure 2-1 illustrates the relationship of the four ERKC phases with the CPIC, SDLC, and C&A processes. (Note: the CPIC, SDLC, and C&A products shown in the figure are limited to those of apparent value in supporting the ERKC process.)

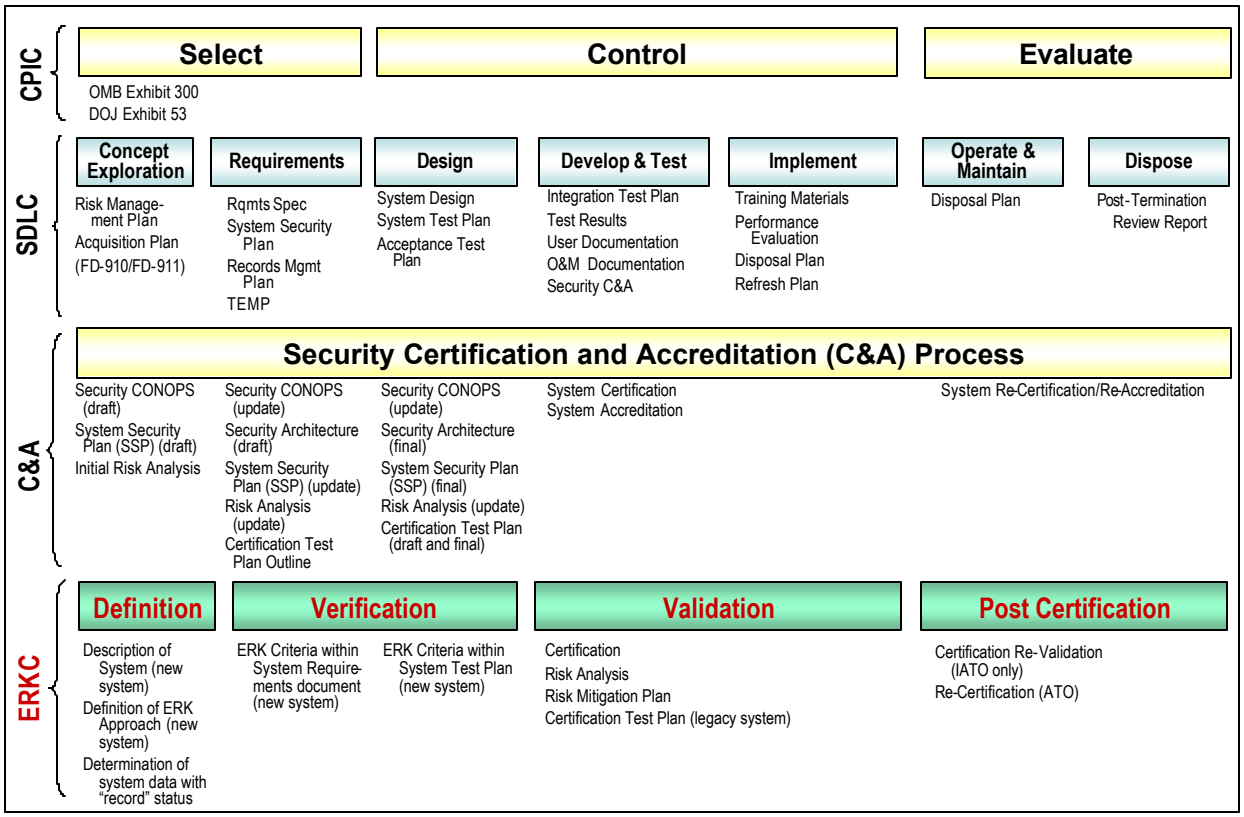


Figure 2-1. The ERKC Process Relationship with Other IT Management Processes

As shown in Figure 2-1, there are four principal phases to the ERKC process, as described immediately below.

2.1.1 Phase 1: Definition

In this phase, once the system has been determined to contain records, the focus is on understanding the ERK approach that will be applied to a system. As noted earlier, there are four primary approaches to achieving ERK certification. Each is described in more detail below. During this phase, the RO may provide advice to the System Owner as the latter determines the specific approach that he or she will take with the system. This advice is an optional service to the System Owner. In addition, the Records Management Division (RMD) of FBI Headquarters will make available guidance on specific ERK criteria and additional guidance on achieving ERK Certification. Appendix C contains the ERK Assessment Criteria.

2.1.1.1 Integration

One approach is to integrate a DoD 5015.2-certified RMA with the system. The National Archives and Records Administration (NARA) endorses the Department of Defense *Electronic Records Management Software Application Design Criteria Standard* (DoD 5015.2-STD, June 2002) for use by all Federal agencies. NARA has evaluated the DoD standard for electronic recordkeeping functionality and has determined that DoD-certified products comply with the relevant provisions of the *Federal Records Act* and NARA regulations with respect to the creation, maintenance and use, and disposition of Federal records. This approach allows for the management of the records as records within the system.

2.1.1.2 Direct Export

Another approach is to design the system such that it will export records directly to an existing Bureau records management application (RMA). This approach is in keeping with the Bureau's Enterprise Architecture (EA), approved by the Director in November 2002.

2.1.1.3 Integral

A third approach is to build into the design of the system or application all of the necessary electronic recordkeeping functionality so as to enable the management of the records as records within the system. This approach would require designing and coding in all of the Bureau's ERK criteria.

2.1.1.4 Deferred

The final approach—designed for emergency or tactical situations only—is to proceed with system development and implementation, with an interim approval to operate (IATO), and then determine whether to (1) dispose of the system and transfer all of the appropriate records to an FBI-approved RMA or (2) request certification of the system, following one of the three other approaches, if the system will have continuing use in the future.

2.1.2 Phase 2: Verification

During this phase, the primary focus is on ensuring that the system design is incorporating the appropriate electronic recordkeeping criteria and is ready for the validation testing that will grant

the system its approval to operate. In the Verification phase, the System Owner will develop a system requirements document (ideally, one that explicitly incorporates ERK criteria) as well as the Test Plan that will include the appropriate test conditions to ensure that ERK criteria are met. Here again, the RO may provide optional assistance in the form of reviewing both the system requirements document as well as the proposed Test Plan to ensure that all appropriate ERK criteria have been included within these early system development documents.

2.1.3 Phase 3: Validation

It is during this phase that the RO validates whether the system seeking ERKC sufficiently satisfies ERK criteria and can be certified. Such certification can take the form of an Approval to Operate (ATO) or an Interim Approval to Operate (IATO), the latter of which grants a temporary approval to operate the system under defined terms and conditions. For example, a legacy system that is scheduled for retirement may be granted an IATO under the condition that it be retired within a specified period of time. Similarly, a system (either new or legacy) may be granted an IATO if it does not meet all of the ERK criteria, but a subsequent risk analysis determines that the risks associated with failing to meet these criteria are "low" or within the bounds of acceptable risk. As explained later in the document, the risk analysis process may require that the System Owner prepare a risk mitigation plan (RMP) as part of the Validation phase.

2.1.4 Phase 4: Post Certification

This phase starts after a system has received a certification (either ATO or IATO) and is intended to ensure the continued "safe" operation of the system (from a recordkeeping perspective). There are two primary activities during this phase: reviewing the status of IATOs and re-certifying systems granted ATOs every three years. In the first case, the RO reviews the terms and conditions specified in the IATO and determines whether the system should be (1) certified with an ATO, (2) issued another IATO to permit further continued operation under defined terms and conditions, or (3) refused further permission to operate [i.e., given No Approval to Operate (NATO)]. In the second case, the RO reviews the system to ensure that its continued operation meets the ERK criteria. The review of ATOs is intended to ensure that no changes have been made that would invalidate a system's continuing ability to satisfy ERK criteria.

2.2 ERKC Process for New Systems

The ERKC process for new systems requires that System Owners and the RO undertake activities in all four phases of the ERKC lifecycle. The sections below describe these activities and provide a simplified "checklist" approach that outlines who does what and who must produce certain written products to support the certification process. Appendix D provides a graphical process-flow model of the ERKC activities for new systems.

2.2.1 Definition Phase

The Definition Phase begins when the RO becomes aware of the planned existence of a new system. The process may be triggered by the flow of certain documentation (e.g., business plans in the form of Exhibit 300s or Exhibit 53s, system security plans, or application architectures) through the RMD at Headquarters and through analogous organizations in FBI field offices.

Once aware of the system, the RO will work with the System Owner to determine whether or not the system will contain records. If not, the process stops and the RO will make an entry into the RMD database with a basic description of the system along with the fact that it will not contain records.

If the system will contain records, the System Owner must determine the system approach for meeting the ERK criteria (i.e., Integration, Direct Export, Integral, Deferred, as described in Section 1.4). RMD personnel are available to advise the System Owner on the benefits and drawbacks of each approach. The System Owner may also access the RMD Web page on the FBI intranet to review ERK criteria and ERKC guidance documents. Once the System Owner has determined an approach, he or she will document that approach in a written notice to RMD.

Table 2-1 illustrates the steps to the Definition phase, including who is responsible for each action and what products (if any) must be produced at each step by each party (i.e., Records Officer or System Owner).

Table 2-1. ERKC Definition Phase - New System

New System ERKC Definition Phase: Activities and Products			
Records Officer		**System Owner**	
Activity	***Product***	***Activity***	***Product***
1. Review available system documentation (e.g., Exhibit 300s, Exhibit 53s, System Security Plans, Application Architectures) to identify new systems.	System logged into RMD ERKC tracking database		
2. Meet with System Owner to determine whether system will contain records. If NO, return to step 1; if YES proceed to Step 3.	Description of system for inclusion within RMD database, and indication of whether system contains records	2. Meet with RO to determine whether system will contain records. If NO, STOP; if YES, proceed to Step 3.	
3. Assist System Owner to establish ERK approach *(as requested by System Owner).*	Logged indication of planned ERK approach	3. Establish ERK approach.	Written notice to RO of ERK approach to be taken

2.2.2 Verification Phase

The Verification Phase follows the Definition Phase and its purpose is to ensure inclusion of ERK criteria into system requirements specifications and test plans that will enable the system to meet ERK criteria when it undergoes subsequent integration and acceptance testing. Table 2-2 illustrates the steps and products associated with this phase. The ERK Assessment Criteria, along with sample tests and expected results, are provided in Appendix C.

Table 2-2. ERKC Verification Phase - New System

New System ERKC Verification Phase: Activities and Products			
Records Officer		**System Owner**	
Activity	***Product***	***Activity***	***Product***
4. Assist System Owner to understand ERK criteria *(as requested by System Owner)*.		4. Understand ERK criteria sufficiently to develop system requirements.	Requirements specifications addressing ERK criteria
5. Assist System Owner to incorporate necessary ERK criteria into System Requirements documentation *(as requested by System Owner)*.	Comments and recommendations on System Requirements documentation *(on request of System Owner)*	5. Develop System Requirements documentation, incorporating necessary ERK criteria.	System Requirements documentation addressing ERK criteria
6. Assist System Owner to incorporate necessary ERK criteria into Test Plan *(as requested by System Owner)*.	Comments and recommendations on Test Plan *(on request of System Owner)*	6. Develop the Integration Test Plan, incorporating necessary ERK criteria.	Test Plan

2.2.3 Validation Phase

Following development of the Test Plan, the Validation phase begins. During this phase, the System Owner will conduct integration/acceptance testing in accordance with the Test Plan developed during the 'Develop and Test' phase of the SDLC. The RO will review the results of that testing to validate compliance with ERK criteria. The RO will then produce a system certification report that identifies all areas of non-compliance. A template for development of an ERK System Certification Report is presented in Appendix J. The RO may need to conduct a risk analysis and the System Owner may need to prepare a risk mitigation plan (also know as an action plan) if full compliance is not evidenced. Information on conducting a risk analysis is located in Appendix F. Table 2-3 illustrates the steps and products associated with the Validation phase.

Table 2-3. ERKC Validation Phase - New System

New System ERKC Validation Phase: Activities and Products			
Records Officer		**System Owner**	
Activity	***Product***	***Activity***	***Product***
7. Support integration/ acceptance testing *(as requested by the System Owner)*.	Comments and recommendations on conduct of integration/acceptance testing *(as requested by the System Owner)*.	7. Conduct the integration/ acceptance testing and document the results of the test; provide a copy of the results to the RO.	Test Results
8. Review test results and determine whether all ERK criteria have been met. If YES, certify the system by granting an ATO; proceed to Step 11 (*Post Certification phase*).	If YES, System Certification Report and ATO. If NO, System Certification	8. If YES, proceed to operate the system; go to Step 11 (*Post Certification phase*). If NO, proceed to step 9	

New System ERKC Validation Phase: Activities and Products			
Records Officer		**System Owner**	
Activity	***Product***	***Activity***	***Product***
If NO, proceed to Step 9.	Report.		
9. Perform a Risk Analysis; determine whether existing risks are acceptable. If YES, issue an IATO; proceed to Step 11 (*Post Certification phase*). If NO, direct System Owner to prepare a Risk Mitigation Plan; proceed to next step.	If YES, IATO. If NO, request preparation of Risk Mitigation Plan.	9. If YES, operate system under terms of IATO; proceed to Step 11 (*Post Certification phase*). If NO, prepare Risk Mitigation Plan; proceed to next step.	If YES, written acknowledge-ment of terms of IATO (to be provided to RO). If NO, Risk Mitigation Plan.
10. Examine Risk Mitigation Plan and determine its feasibility. If plan is feasible (i.e., YES), pro-ceed to next step. If plan is not feasible (i.e., NO), issue NATO; STOP.	Determination on feasibility of Risk Mitigation Plan. If YES, IATO If NO, NATO.	10. If YES, proceed to next step.	If YES, written acknowledgement of terms of IATO (to be provided to RO). If NO, revise mitigation plan.

2.2.4 Post Certification Phase

There are two primary purposes of the Post Certification phase. The first is to enable the RO to determine whether the terms of any IATO should be extended, or whether the IATO should be changed to an ATO, or to a NATO. The second is to perform routine, periodic (every three years) reviews of the status of systems granted ATOs to ensure that such systems continue to meet all ERK criteria.

Each IATO issued by the RO will have certain terms and conditions associated with it. For example, the IATO may authorize operations of a system (not fully compliant with electronic recordkeeping requirements) for a specified period of time (e.g., 12 months). The RO may issue such an IATO to accommodate the development of a system following a spiral development process in which all of the required electronic recordkeeping criteria are not expected to be satisfied until the second release. Or, an IATO may be intended to accommodate the development and implementation of a system put in place to meet emergency operational needs (e.g., the tracking system used in response to the Washington metropolitan-area sniping incident in the fall of 2003). Similarly, an IATO may authorize the operation of a system in a restricted operational environment (e.g., on a separate local area network not connected to the FBI intranet) to serve as a proof of concept before implementing its fully ERK-compliant counterpart on a broader scale.

Regardless of the terms and conditions associated with the IATO, the intent of the Post Certification phase is to examine the operation of the system covered by the IATO and determine the next appropriate step to be taken. In the above hypothetical example of a system following a spiral development methodology, with the implementation of the second release, the appropriate action may be to convert the IATO to an ATO. In the case of a system developed for emergency operational needs, the appropriate action may be to disallow continued operations (e.g., the

emergency is over) and require all of the records created within the system to be transferred to an approved RMA.

With respect to systems granted ATOs, the RO must review the operations of such systems every three years to ensure continuing compliance with ERK criteria. Once granted an ATO, a system may undergo changes (e.g., new functionality) that could cause the system to no longer satisfy the ERK criteria. In such cases, the RO may require further modifications to the system in order to accommodate these ERK criteria.

Table 2-4 illustrates the steps and products associated with the Post Certification phase.

Table 2-4. ERKC Post Certification Phase - New System

New System ERKC Post Certification Phase: Activities and Products			
Records Officer		**System Owner**	
Activity	***Product***	***Activity***	***Product***
11. Monitor ATO and IATO expiration dates.		11. Operate system under terms and conditions of the granted ATO or IATO.	
12 Notify System Owner of re-certification	Re-certification Notice	12. Provide relevant documentation	If ATO, provide requirements specifications for new functionality (since last ERK certification) If IATO, provide evidence (requirements specification/test results) of compliance with conditions of IATO.
13. Review documentation and determine whether all ERK criteria have been met. If YES, certify the system by granting an ATO; proceed to Step 11 (*Post Certification phase*). If NO, proceed to Step 14.	If YES, System Certification Report and ATO. If NO, System Certification Report., proceed to step 14.	13. Support RO review of documentation. If YES, continue to operate the system; go to Step 11 (*Post Certification phase*). If NO, proceed to step 14	
14. Perform a Risk Analysis; determine whether existing risks are acceptable. If YES, issue an IATO; proceed to Step 11 (*Post Certification phase*). If NO, direct System Owner to prepare a Risk Mitigation Plan; proceed to next step.	If YES, IATO. If NO, request preparation of Risk Mitigation Plan.	14. If YES, operate system under terms of IATO; proceed to Step 11 (*Post Certification phase*). If NO, prepare Risk Mitigation Plan; proceed to next step.	If YES, written acknowledge-ment of terms of IATO (to be provided to RO). If NO, Risk Mitigation Plan.

New System ERKC Post Certification Phase: Activities and Products			
Records Officer		**System Owner**	
Activity	***Product***	***Activity***	***Product***
15. Examine Risk Mitigation Plan and determine its feasibility	Determination on feasibility of Risk Mitigation Plan. If YES, IATO If NO, NATO.	15. Review mitigation plan with RO	If YES, written acknowledgement of terms of IATO (to be provided to RO). If NO, revise mitigation plan.

2.3 ERKC Process for Legacy Systems

The ERKC process for legacy systems requires that System Owners and the RO undertake activities in only the last two phases of the ERKC lifecycle because such systems have already been developed and undergone integration and acceptance testing (most likely without regard to electronic recordkeeping requirements). The sections below describe the associated activities and provide a simplified "checklist" approach that outlines who does what and who must produce certain written products to support the certification process. (Appendix E provides a graphical process-flow model of the ERKC activities for legacy systems.) Because integration and acceptance testing will have already occurred for legacy systems, it may be necessary to develop and conduct a special certification test (validation by demonstration) if the RO is unable to determine from a review of existing system documentation[4] whether the system complies with ERK criteria.

2.3.1 Validation Phase

The purpose of the Validation phase for legacy systems is to determine whether the system satisfies the ERK Assessment Criteria, presented in Appendix C. The RO will attempt to ascertain this fact by reviewing various documents associated with the system. If sufficient information is not available, the RO will request the conduct of a specially focused certification test.

The RO will initiate the ERKC process whenever he or she becomes aware of a legacy system. Triggers include Exhibit 300s and 53s, revisions to system security plans, and updates to application architecture documents. The RO will work with the System Owner to determine whether the system contains records. If the system does not contain records, no further action by the System Owner is required - the RO documents this fact in the RMD database discussed earlier in section 2.2.1.

If the system does contain records, the RO will attempt to determine whether the system meets all necessary ERK criteria by reviewing the results of the system's integration/acceptance testing. If an appropriate determination cannot be made from these test results, the RO will request additional documentation (e.g., user's manuals, system administration manuals). If the RO still cannot determine whether the system satisfies the needed ERK criteria, the RO will direct the System Owner to develop and conduct a special certification test for the system. From this point on, the System Owner and the RO will follow the same process described in Section

[4] Existing documentation may include, but is not limited to, test plans, system design documents, requirements specifications, user's manuals and system administration manuals.

2.2.3 for the Validation phase for a new system. As noted in Section 2.2.3, this process may require the RO to conduct a risk analysis and the System Owner to prepare a risk mitigation plan. Table 2-5 illustrates the steps and products associated with the Validation phase for a legacy system.

Table 2-5. ERKC Validation Phase - Legacy System

Legacy System ERKC Validation Phase: Activities and Products			
Records Officer		**System Owner**	
Activity	***Product***	***Activity***	***Product***
1. Review available system documentation (e.g., Exhibit 300s, Exhibit 53s, System Security Plans, Application Architectures) to identify legacy systems.	System logged into RMD ERKC tracking database		
2. Meet with System Owner to determine whether system contains records. If YES proceed to Step 3.	Description of system for inclusion within RMD database, and indication of whether system contains records	2. Meet with RO to determine whether system contains records. If YES, proceed to Step 3.	
3. Request Requirements Specifications, Test Plans, and test results from system integration/acceptance testing.	Request for System documentation.	3. Provide System Documentation (as available)	System documentation.
4. Review System Documentation to determine whether ERK criteria are being met	System Certification Report. If YES, ATO If NO, go to Step 5.		
5. If documentation is insufficient to evidence compliance, validate ERK criteria by demonstration	Updated System Certification Report	5. Demonstrate relevant system functionality in support of ERKC evaluation.	System demonstration.
6. Review System Certification Report and determine whether all ERK criteria have been met. If NO, proceed to Step 14.	If YES, ATO. If NO, proceed to next step.	6. If YES, continue to operate the system; go to Step 11 (*Post Certification phase*). If NO, proceed to next step	
7. Perform a Risk Analysis; determine whether existing risks are acceptable. If YES, issue an ATO; If NO, direct System Owner to prepare a Risk Mitigation Plan; proceed to next step.	If YES, ATO. If NO, request preparation of Risk Mitigation Plan.	7. If YES, operate system If NO, prepare Risk Mitigation Plan; proceed to next step.	If YES, written acknowledge-ment of terms of ATO (to be provided to RO). If NO, Risk Mitigation Plan.

Legacy System ERKC Validation Phase: Activities and Products			
Records Officer		**System Owner**	
Activity	***Product***	***Activity***	***Product***
8. Examine Risk Mitigation Plan and determine its feasibility	Determination on feasibility of Risk Mitigation Plan. If YES, IATO If NO, NATO.	8. Review mitigation plan with RO	If YES, written acknowledgement of terms of IATO (to be provided to RO). If NO, revise mitigation plan.

2.3.2 Post Certification Phase

The purpose of the Post Certification phase for a legacy system is twofold. First, it is to enable the RO to determine whether the terms of any IATO should be extended or whether the IATO should be changed to an ATO or to a NATO. Second, it is to enable the RO to perform routine, periodic (every three years) reviews of the status of systems granted ATOs to ensure that such systems continue to meet all ERK criteria.

IATOs for legacy systems will have certain terms and conditions associated with them. For example, an IATO may authorize the continued operations of a non-ERK-compliant system for a specified period of time (e.g., 12 months) because that system will be retired or replaced with an ERK-compliant system within that period of time and the costs of retrofitting the non-compliant system are deemed excessive relative to the risks associated with its continued as-is operations. Similarly, the RO may issue an IATO for a legacy system because there is a planned upgrade to the system that will make it ERK-compliant within a specified period of time. Lastly, the RO may issue an IATO for a legacy system because it was developed and implemented for emergency purposes and the emergency situation still exists. The process for post-certification of legacy systems, however, is identical to the post-certification process described for new systems. This process is described in detail in Table 2-4.

❖ ❖ ❖

Section Three—Roles and Responsibilities

This section summarizes the primary roles and responsibilities of the two principal participants in the electronic recordkeeping certification (ERKC) process. Section 3.1 highlights the responsibilities of the Records Officer (RO). Section 3.2 summarizes the responsibilities of the System Owner.

3.1 Records Officer ERKC Responsibilities

The principal role of the RO is to determine whether FBI IT systems contain records. If so, the RO certifies whether the system meets the FBI criteria for an ERK system. In performing ERKC activities, the Records Officer shall execute the following responsibilities:

- Develop, publish, and maintain, on the RMD page of the FBI intranet, ERK criteria associated with the four defined approaches to meeting ERK criteria (i.e., Integration, Direct Export, Integral, Deferred).
- Determine, in consultation with System Owners, whether a system contains records (legacy systems) or will contain records once implemented (new systems).
- As requested by System Owners, provide advice and guidance to System Owners when they are selecting their preferred approach to meeting ERK criteria.
- As requested by System Owners, provide advice and guidance on the ERK certification content of System Owner-developed Test Plans.
- As requested by System Owners, provide assistance on the conduct of the ERK certification portions of Test Plans.
- Review and evaluate the results of Test Plans, or other relevant system documentation, from an ERK certification perspective, and report results of the ERK certification evaluation.
- For legacy systems, determine whether validation by demonstration is required, and notify System Owners of the requirement.
- Perform risk analyses, as needed, for systems to determine whether the risks posed by systems not meeting all ERK criteria are acceptable risks.
- Direct System Owners to prepare Risk Mitigation Plans for systems not meeting all ERK requirements that pose unacceptable risks; determine the feasibility of successfully executing such Risk Mitigation Plans and so notify System Owners.
- Determine the appropriate certification [i.e., Approval to Operate (ATO), Interim Approval to Operate (IATO), and No Approval to Operate (NATO)] for each system that comes under his or her cognizance.
- Review systems operating under the terms and conditions of an IATO and determine whether to issue an ATO, extend the terms of the IATO, or issue a NATO.
- Review systems operating under ATOs every three years and determine whether to grant re-certification for such systems (new ATO), issue an IATO, or issue a NATO.

3.2 System Owner ERKC Responsibilities

The System Owner's role is to ensure that FBI IT systems for which they are responsible meet the FBI ERK criteria. In operating their systems and participating in ERKC activities, System Owners shall execute the following responsibilities:

- Notify the RO of all planned new systems and existing legacy systems.
- Meet with the RO, when requested, to help determine whether systems contain records.
- Establish the appropriate ERK approach for each system owned or operated by the System Owner.
- For new systems, develop and incorporate the appropriate ERK criteria into the system requirements specifications and integration/acceptance Test Plans (in consultation with the RO, if so desired).
- Conduct system integration/acceptance testing according to Test Plans containing appropriate ERK criteria.
- Provide standard system documentation (e.g., user's manuals, system administration manuals, system design documents), as requested by the RO, to support the ERKC process.
- Provide the results of (1) integration/acceptance tests and, as appropriate, (2) ERKC tests to the RO.
- When requested by the RO, develop Risk Mitigation Plans for systems.
- Notify the RO of planned changes to any system operating under an ATO that might adversely affect the ERK certification of that system.
- Comply with the terms and conditions of the appropriate certification (i.e., ATO, IATO, and NATO) for each system that is operated.
- Cooperate with the RO in the review and re-certification activities (every three years) for each system granted an ATO.

❖ ❖ ❖

Appendix A—References

Basic Functional Requirements for Electronic Recordkeeping (ERK) for Automated Systems/ Applications in the FBI, FBI, draft of March 3, 2003

Design Criteria Standards for Electronic Records Management Software Applications, DoD 5015.2-STD, June 19, 2002

FBI Certification and Accreditation Handbook, FBI, Version 1.1, July 31, 2003

FBI Enterprise Records Management Application: High-Level Functional Requirements, FBI, 66F-HQ-C14032470-5, Revised February 2003

Framework for Integration of Electronic Document Management and Electronic Records Management Systems, ANSI/AIIM/ARMA TR 48-200X Technical Report for Information and Image Management, expected publish date June 2004

Management of Federal Information Resources, OMB Circular A-130, November 28, 2000

Program Management Office Functional Overview, PMO-PLN-001, Version 1.0, FBI, June 2003

Records Management Division Delegation of Authority to the Agency Records Officer, FBI, 66F-HQ-A1358157-32, April 29, 2002

U.S. National Archives and Records Administration (NARA) Fast Track Project, http://www.archives.gov/records_management/policy_and_guidance/fast_track.html

36 CFR § 1220 to 1238 (Records Management).

44 U.S.C. § 29 (Records Management by the Archivist of the United States and the Administrator of General Services).

44 U.S.C. § 31 (Records Management by Federal Agencies).

❖ ❖ ❖

Appendix B—Glossary

Acronyms

Abbreviation	Meaning
ATO	Approval to operate
C&A	Certification and Accreditation
CFR	Code of Federal Regulations
CPIC	Capital Planning and Investment Control
DoD	Department of Defense
EA	Enterprise Architecture
ERK	Electronic recordkeeping
ERKC	Electronic recordkeeping certification
FBI	Federal Bureau of Investigation
IATO	Interim approval to operate
ID	Identification *(as in User ID)*
IDW	Investigative Data Warehouse
IRM	Information resource management
IS	Information system
IT	Information technology
KM	Knowledge management
NARA	National Archives and Records Administration
NATO	No approval to operate
OMB	Office of Management and Budget
RM	Records management
RMA	Records management application
RMD	Records Management Division
RMP	Risk mitigation plan
RO	Records Officer
SDLC	System Development Life Cycle
U.S.C.	United States code
VCF	Virtual Case File

Terms

Term	Definition
Approval to operate	Certification to operate a system on a "permanent" basis (in the absence of subsequent modifications to the system); granted by the Records Officer. Each ATO is good for a period of three years and the System Owner must seek re-certification for each system operating under an ATO within the 3-year window that begins upon the granting of an ATO for that system.
Category	A category is a records series, or a group of records with similar characteristics assigned to a particular records retention schedule and generally handled as a unit for disposition purposes. In many RMAs, a category is a file folder icon in which records are assigned.
Disposition instructions	Those actions taken regarding Federal records after they are no longer required to conduct current Agency business. These actions include: 1) transfer of records to Agency storage facilities or Federal Record Centers (FRCs); 2) transfer of records from one Federal Agency to another; 3) transfer of permanent records to the National Archives; 4) disposal of temporary records, usually by destruction.
Exact match search	Exact-match searches return data that include the exact search string; also known as "on-the-nose" search.
File Plan	A file plan is a document containing the identifying number, title or description and disposition authority of files held or used in an office.
Global change	A global change is an automatic search-and-replace feature. Global changes are performed when one change needs to be made to a number of records. By doing a global change, the new data is keystroked once.
Investigative Data Warehouse	A portal to various FBI databases and documents that includes a workflow process and search capabilities for the purpose of discovering knowledge.
Interim approval to operate	Certification to operate a system for a temporary period of time and subject to specified conditions; granted by the Records Officer.
Metadata	Metadata is structured data about data; it is a term that describes or specifies characteristics that need to be known about data in order to build information resources such as ERK systems and support records creators and users.
Proximity searching	Proximity or adjacency searches return data that include search strings within a certain "distance" of other strings, e.g., when the word "fire" is within 50 characters of "explosion."

Terms

Record	Documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the FBI.
Risk analysis	The process performed by the RO to determine the acceptability of the risks posed by a system that does not meet all of the required ERK criteria.
Records Officer	The designated individual responsible for reviewing the ERK capabilities of systems (both legacy and new) and determining whether to grant the System Owner permission to operate that system from a recordkeeping perspective.
Relevance ranking	Relevance ranking is a system mechanism that determines the degree to which the retrieved data are relevant to the search.
Risk mitigation plan	A plan developed by the System Owner that spells out a proposed approach to alleviate the risks posed by a system that does not meet all ERK criteria.
Sealed Records	Sealed records are those that have been redacted, and have an identifying border burned into the document so that redacted information may not be reverse engineered. Sealed documents may not be unsealed.
Stop words	Stop words are extremely common words that a search engine will not search for in order to save space or to speed up searches. Examples include: "the," “it,” “and,” “a," “or,” etc.
System owner	The individual with responsibility for developing or operating an FBI information or knowledge management system.
Unmet ERK criteria	A set of ERK criteria, determined by the RO, for a system undergoing ERKC that the system fails to satisfy.
Virtual Case File	The electronic repository of case file records, which includes a records management system operated by the FBI that meets FBI records management requirements.
Vital Record	Vital records are those needed by agencies for continuity of operations before, during, and after emergencies, and those records needed to protect the legal and financial rights of the Government and persons affected by Government activities.
Wildcard characters	Wildcard characters can be used in queries in place of unknown characters and to search for multiple variations of a term. For example, searching on “terror*” would retrieve data that include “terror,” “terrorist,” “terrorism,” etc.

Appendix C—ERK Assessment Criteria

Appendix C contains the ERK assessment criteria that have been established by the Records Management Division for all FBI recordkeeping information systems. The criteria are the basis for which new and existing systems are evaluated for electronic recordkeeping certification. Each criterion is followed by one or more sample tests and expected results that can be used to assist System Owners in developing test plans and to support the review of test results by Records Officers. NOTE: The "user" refers to authorized users only. Different functions are permitted to different groups of users – e.g., administrative functions to records managers, retrieval functions to end-users, etc.

1.1 Declare Records

Criterion 1.1.1: The system designates specified information as records, either manually or automatically.

Sample Test(s)	Expected Result(s)
Import a document into the system. Designate the document as a record.	The document is marked/flagged as a record in its metadata Other documents in the system not designated as records are not marked/flagged as records in their metadata.

Criterion 1.1.2: The system assigns unique identifiers to records and their associated metadata.[5] The system prevents any modification of a record's unique identifier, once it is defined.

Sample Test(s)	Expected Result(s)
Attempt to assign a common ID to two records.	The system generates a notification to the user that this task is prohibited, and prevents assigning a common ID to two distinct records.
Assign unique IDs to a set of records and their associated metadata. Check whether the IDs adhered to the records and their associated metadata.	Assigned IDs adhered to the records and their associated metadata.
Attempt to modify or delete assigned IDs.	The system generates a notification to the user that this task is prohibited, and prevents modifying and deleting assigned IDs.

Criterion 1.1.3: The system captures record metadata (FBI-designated and others) automatically and reliably links metadata to the records.

Sample Test(s)	Expected Result(s)
For a record, retrieve each of the FBI-designated metadata elements.	Each FBI-designated metadata element is retrieved and populated with a valid entry.

1.2 Capture Records

Criterion 1.2.1: The system imports records from sources outside the system (e.g., other information systems, desktop applications, scanned documents, or e-mail) along with all required associated metadata (e.g., records series, pre-existing file plans[6], or locations for physical records)

[5] Metadata is structured data about data; it is a term that describes or specifies characteristics that need to be known about data in order to build information resources such as ERK systems and support records creators and users.
[6] A file plan is a document containing the identifying number, title or description and disposition authority of files held or used in an office.

Sample Test(s)	Expected Result(s)
Import a record and its associated metadata into the system from a desktop management system.	The record and its associated metadata are successfully imported into the system.
Criterion 1.2.2: To provide records management control over the records without physically transporting them to an RMA, the system links records to an external RMA.	
Sample Test(s)	**Expected Result(s)**
Flag an entity in the system as a record and link it to the relevant file classification in the RMA.	The entity is identified in the system as a record and linked to the appropriate file classification and disposition existing in the RMA; RMA treats the record as a record.
1.3 MAINTAIN OR USE RECORDS **1.3.1 Record Organization**	
Criterion 1.3.1.1: The system accepts an FBI-specific scheme for organizing records. For example, the system accepts FBI-specific records retention schedules and organizes records according to the schedules.	
Sample Test(s)	**Expected Result(s)**
Input an FBI-specific records retention schedule to the system. Input information declared as records with pre-known records retention schedule characteristics. Process and output records according to the records retention schedule.	FBI-specific records retention schedule is successfully input to the system. Information input to the system is output as records with correct records retention schedule characteristics.
Criterion 1.3.1.2: Users can select categories[7] in which records are filed and assign records to these categories.	
Sample Test(s)	**Expected Result(s)**
Input a user-designated file plan category. Assign records to the user-designated file plan category.	User-designated file plan category conflicting with FBI-specific file plan is rejected. User-designated file plan category not conflict with FBI-specific file plan is accepted. Records assigned to the user-designated file plan category are contained within or linked to the category.
Criterion 1.3.1.3: The system supports assignment of Vital Record[8] indicators.	
Sample Test(s)	**Expected Result(s)**
Input information that is a known Vital Record. Designate the information as a Vital Record by assigning a "yes" value to the Vital Record metadata element	Record is shown as Vital Record in its metadata.
Criterion 1.3.1.4: The system supports linking of related records (e.g., a redacted record with its non-redacted counterpart, an original record with its revision, or an electronic record with a paper antecedent[9]).	

[7] A category is a records series, or a group of records with similar characteristics assigned to a particular records retention schedule and generally handled as a unit for disposition purposes. In many RMAs, a category is a file folder icon in which records are assigned.

[8] Vital records are those needed by agencies for continuity of operations before, during, and after emergencies, and those records needed to protect the legal and financial rights of the Government and persons affected by Government activities.

[9] For example, an official correspondence may have been initiated on paper (paper antecedent), and the response was an electronic reply (electronic record).

Sample Test(s)	Expected Result(s)
Perform operation of linking records with other related records.	Record metadata carry information that designates other records to which they are linked.
Criterion 1.3.1.5: The system supports the capability for users to create and edit file plans, including categories and sub-categories. The system prevents deletion of non-empty folders.	
Sample Test(s)	**Expected Result(s)**
Create a system file plan and a category and sub-category within the file plan. Edit the file plan, category and sub-category. Delete the file plan, category and sub-category. Attempt to delete a category containing items.	Categories and sub-categories are successful created, edited and deleted in the system file plan. The system generates a notification to the user that this task is prohibited, and prevents deletion of the category containing items.
Criterion 1.3.1.6: The system can assign a status to records to prevent destruction (i.e., the system contains an indicator that includes an option to mark records as "do-not-destroy," which prevents records from being selected for destruction or transfer according to records retention schedules).	
Sample Test(s)	**Expected Result(s)**
Select the "do-not-destroy" status for a record that is identified for destruction according to the records retention schedule. Attempt to identify the record for destruction while the "do-not-destroy" status is selected.	The "do-not-destroy" status is visible and enabled for the record. Unsuccessful in identifying the record for destruction.
Criterion 1.3.1.7: The system supports global[10] changes to metadata, file plans, and records retention schedules.	
Sample Test(s)	**Expected Result(s)**
Change the value of a metadata element from its current value to another using a single keystroke.	All instances of the former value are changed to the new value. No instances of the former value remain in the selected metadata element.
Criterion 1.3.1.8: The system executes disposition[11] instructions (e.g., moves a group of records from active to inactive status or designates a group of records for destruction or transfer).	
Sample Test(s)	**Expected Result(s)**
Search the system for a set of records that are eligible for disposition. Use authorized user ID to approve and execute the disposition instructions for the set of records Use unauthorized user ID to attempt to approve and execute the disposition instructions for the set of records.	System identifies and lists the set of records that are eligible for disposition The disposition instructions are successfully executed under the authorized user ID. The system generates a notification to the user that this task is prohibited, and prevents execution of disposition instructions under the unauthorized user ID.

[10] A global change is an automatic search-and-replace feature. Global changes are performed when one change needs to be made to a number of records. By doing a global change, the new data is keystroked once.

[11] Those actions taken regarding Federal records after they are no longer required to conduct current Agency business. These actions include: 1) transfer of records to Agency storage facilities or Federal Record Centers (FRCs); 2) transfer of records from one Federal Agency to another; 3) transfer of permanent records to the National Archives; 4) disposal of temporary records, usually by destruction.

Criterion 1.3.1.9: For systems that manage physical records, the system specifies identifiers for boxes, contents, locations, etc. In other words, the system stores metadata for records not contained in the system and can identify records by physical location (box number, location ID, etc.)	
Sample Test(s)	**Expected Result(s)**
Enter in the system physical location metadata for a physical record.	Metadata for the physical record is accepted and stored in the system.

1.3 MAINTAIN OR USE RECORDS
1.3.2 Records Security

Criterion 1.3.2.1: The system prevents over-writing records. To comply with records management guidelines, records are never edited, but new versions are created and linked to the source.	
Sample Test(s)	**Expected Result(s)**
Copy a record from the system to a document management application. Modify the record and attempt to re-file it in the system.	Record copy is created and accessible in the document management system. System prevents the modified record to overwrite the original record. System prompts the user to file the modified record as a new record.
Criterion 1.3.2.2: The system prevents deletion of indices, categories, and other 'pointers' to records (i.e., maintains referential integrity).	
Sample Test(s)	**Expected Result(s)**
User attempts to modify and/or delete indices and categories for a set of records.	Prohibited action will not happen. Indices or categories in use will not be deleted or modified.
Criterion 1.3.2.3: The system provides an automatic method to detect any alteration of records or metadata.	
Test(s)	**Expected Result(s)**
Verify in system design documentation that changes to records or metadata can be automatically determined by the system. Using an authorized user ID, modify information designated as a record.	The system design documentation indicates that the system automatically determines (e.g., by checksums) when records or metadata have been modified. The system generates a notification of record modification.
Criterion 1.3.2.4: The system provides audit trails of all add, update, deletion, and retrieval activity.	
Sample Test(s)	**Expected Result(s)**
Using an authorized user ID, create, access, edit and delete a record.	The history and audit trail of the record indicates the creation, access, modification and deletion of the record. The history and audit trail are present and accessible in the system.
Criterion 1.3.2.5: The system (or System Owner) maintains appropriate backup copies of records and recordkeeping systems.	
Sample Test(s)	**Expected Result(s)**
Verify that back-up procedures exist for the system.	The system follows its back-up procedures and has a history of being backed up.
Criterion 1.3.2.6: The system is protected by adequate recovery/rollback and rebuild procedures so that records may be recovered or restored following a system malfunction.	
Sample Test(s)	**Expected Result(s)**
Verify that recovery/rollback and rebuild procedures exist for the system.	The system has recovery/rollback and rebuild procedures in place and they have been tested.

1.3 MAINTAIN OR USE RECORDS 1.3.3 Records Access	
Criterion 1.3.3.1: The system controls access so that only authorized individuals are able to retrieve, view, print, copy, or edit records or other entities (e.g., metadata, file plan, etc.) in the recordkeeping system.	
Sample Test(s)	**Expected Result(s)**
Designate a test set of user IDs; set access privileges to retrieve, view, print, copy or edit a record: Use an authorized user ID to retrieve, view, print, copy or edit a record. Use an unauthorized user ID to attempt to retrieve, view, print, copy or edit a record.	Record is able to be retrieved, viewed, printed copied and edited. The system generates a notification to the user these tasks are prohibited, and prevents the actions from occurring.
Criterion 1.3.3.2: The system identifies individuals and groups of users and allows different access privileges to be assigned to individuals or groups.	
Sample Test(s)	**Expected Result(s)**
Designate two test sets of user IDs; give members of each set different access privileges and restrictions. For each set of user IDs, attempt actions that are both allowable and restricted based on the access privileges and restrictions set.	Allowable actions will occur for each set of user IDs. Prohibited actions will not occur for each set of user IDs.
Criterion 1.3.3.3: The system maintains the integrity of redacted records and assures that redacted material is not accessible on sealed[12] records.	
Sample Test(s)	**Expected Result(s)**
Retrieve a random sample of sealed records and verify redacted material is not viewable. Attempt to reconstruct the redacted material.	All redacted material in the sealed records is not viewable. The redacted material cannot be reconstructed.

1.3 MAINTAIN OR USE RECORDS 1.3.4 Records Retrieval	
Criterion 1.3.4.1: The system ensures that all access privileges (permissions and restrictions) are enforced on all retrievals.	
Sample Test(s)	**Expected Result(s)**
Designate a test set of user IDs; set different records retrieval access privileges for each of the IDs: With each user ID, attempt both allowable and prohibited retrievals.	Allowable retrievals will occur. Prohibited retrievals will not occur.
Criterion 1.3.4.2: The system can retrieve records and their associated metadata and can retrieve records based on defined links (e.g., between versions of the same record or between the records in a particular case file).	
Sample Test(s)	**Expected Result(s)**
Simultaneously retrieve both a record and its associated metadata. Define a link among a record and its related records. Then, search the system for this record and all its related (linked) records.	The record and its associated metadata are retrieved in a single search. Links are defined, and the record and all its related records are retrieved in a single search.

[12] Sealed records are those that have been redacted, and have an identifying border burned into the document so that redacted information may not be reverse engineered. Sealed documents may not be unsealed.

Criterion 1.3.4.3:	The system provides a sufficiently powerful range of search features and options, as needed to meet agency requirements. These might include: searching on individual terms or a combination of terms, wildcard[13] or exact-match[14] searching, proximity or adjacency[15] searching, relevance ranking[16] of search results, use of stop words[17], limits on maximum size of results set from a search, query by image content, or others.
Sample Test(s)	**Expected Result(s)**
Conduct records searches by (a) searching on individual terms, (b) searching on a combination of terms, (c) wildcard matching, (d) exact-matching, (e) proximity or adjacency searching, (f) excluding specified stop words, (g) setting limits on the maximum size of the results set, (h) searching image content, and (i) using other functions determined by System Owner as necessary for the system.	All selected search functions are successfully completed. Search results include only those that match the search criteria.
Conduct a search that ranks the search results according to relevance – most relevant search results appearing at the beginning of the list, gradually decreasing in relevance to the bottom of the list.	Search results are listed in order of relevance. System documentation describes the algorithm(s) used to rank search results.

1.3 MAINTAIN OR USE RECORDS
1.3.5 Records Preservation

Criterion 1.3.5.1:	The system provides users the capability to read and accurately interpret all records (and metadata) in the system throughout their useful life. The system has capability to continuously sample older records for the ability to machine-read records and their metadata, and reports failures to machine-read.
Sample Test(s)	**Expected Result(s)**
Set sampling criteria, age, and periodicity parameters for sampling older records (e.g., 1 percent sample of records older than 3 years, run once each week).	System accepts the sampling parameters.
Run sampling process to machine-read sampled records, reporting function, and output function.	System will successfully run the records/metadata sampling process continuously as per instructions.
Ensure system is set for continuous running of sampling process.	System successfully reports machine-readability results for sampling process. System successfully outputs set of older records for human readability.

[13] Wildcard characters can be used in queries in place of unknown characters and to search for multiple variations of a term. For example, searching on "terror*" would retrieve data that include "terror," "terrorist," "terrorism," etc.
[14] Exact-match searches return data that include the exact search string; also known as "on-the-nose" search
[15] Proximity or adjacency searches return data that include search strings within a certain "distance" of other strings, (e.g., when the word "fire" is within 50 characters of "explosion.")
[16] Relevance ranking is a system mechanism that determines the degree to which the retrieved data are relevant to the search.
[17] Stop words are extremely common words that a search engine will not search for in order to save space or to speed up searches. Examples include: "the," "it," "and," "a," "or," etc.

Criterion 1.3.5.2:	The system enables migration of records and metadata to new storage media or formats in a way that the content is retained and understandable in order to avoid loss due to media decay or technology obsolescence.
Sample Test(s)	**Expected Result(s)**
Select a set of records and metadata. Convert the records to the standard FBI software format for migrating records. Export a set of records and metadata to another system and verify receipt of export.	The converted records and metadata are opened successfully in the new software format. The records and metadata content has not changed and remains readable and understandable. Selected set of records and metadata are successfully imported to another system. The records and metadata content has not changed and remains readable and understandable.
Criterion 1.3.5.3:	The system ensures that captured metadata remains linked to appropriate records without alteration throughout the useful life of the records. The system supports the capability to continuously sample records to verify that metadata remain associated with records and to output results of the sampling process.
Sample Test(s)	**Expected Result(s)**
Set sampling criteria and periodicity for sampling records (e.g., 1 percent sample of all records, run once each week). Run sampling process to verify that records remain associated with their metadata. Run reporting function, and output function. Ensure system is set for continuous running of sampling process.	Sampling criteria and periodicity will be successfully set. Sampled records are associated with their metadata. Errors in associating records and metadata are reported System continuously runs the sampling process.

1.3 MAINTAIN OR USE RECORDS
1.3.6 Audit/Oversight

Criterion 1.3.6.1:	The system provides access to summary reports (e.g., number of accesses) and detail level audit trail information (e.g., each individual record access, including record identifier, date, time and user). The system supports the capability to continuously compile and output periodic and on-demand reports of summary and detailed audit trail information.
Sample Test(s)	**Expected Result(s)**
Set formats, data elements, parameters, and periodicity for audit trail reports. Perform, output, and/or provide user access to periodic audit trail report. Perform, output, and/or provide user access to on-demand audit trail report. Set system for continuous running of audit trail report function.	Periodic audit trail reports are successfully compiled and output according to set formats, data elements, parameters, and periodicity. On-demand audit trail reports are successfully output and/or prepared for access. System continuously runs the audit trail report function.
Criterion 1.3.6.2:	The system tracks failed attempts of all records activity and system functions. In other words, the system detects, records and outputs any unsuccessful attempts to access records or metadata, or conduct other system functions. The system tracks information such as user ID, date and time of failed attempts.
Sample Test(s)	**Expected Result(s)**

Using an unauthorized user ID, attempt to modify a record. Using an unauthorized user ID, attempt to modify user access permissions.	Failed attempt at record modification is detected, recorded, and output. Failed attempt at modification of user access permissions is detected, recorded, and output.
Criterion 1.3.6.3: Audit trail information is managed as records in order to prevent editing of audit logs.	
Sample Test(s)	**Expected Result(s)**
Perform set of actions resulting in audit trail activity. Either manually or automatically, declare the audit trail report a record and enter associated metadata. Verify that each audit trail report is declared a record with associated metadata.	Audit trail activity is recorded as expected. Audit trail report is declared a record and its associated metadata is linked to the record.
1.4 DISPOSE OF RECORDS (FINAL) (Transfer or Destroy)	
Criterion 1.4.1: The system identifies records eligible for transfer or destruction based on records retention schedules and disposition instructions (i.e., the system automatically detects when a record's retention period will pass, notifies the Records Officer that the record is eligible for disposition, and stipulates whether the record is eligible for transfer or destruction).	
Sample Test(s)	**Expected Result(s)**
Develop a test set of records in the system that is eligible for disposition tomorrow.	Records Officer is notified by the system that the set of records is eligible for disposition. Records Officer is informed by the system which records are eligible for transfer and which for destruction.
Criterion 1.4.2: The system exports records and metadata to be transferred (i.e., copy and subsequently remove them from the system) in a format acceptable for transfer to NARA[18].	
Sample Test(s)	**Expected Result(s)**
Verify in system documentation that records can be exported in NARA-accepted formats. Issue export command for a set of records.	Records are copied to an outside system or media; in NARA-acceptable formats.
Criterion 1.4.3: The system deletes records to be destroyed so they cannot be physically reconstructed or otherwise retrieved.	
Sample Test(s)	**Expected Result(s)**
Insert set of records and metadata to be destroyed. Issue destruction command for the records and metadata. Attempt to retrieve and reconstruct the records and metadata.	Designated records and metadata are deleted from the system. Neither the system nor any external procedures or software is successful in retrieving or reconstructing the records and metadata.
Criterion 1.4.4: The system maintains a record of all record transfers and destructions and provides certifiable proof of transfer or destruction. All records of transfer or destruction are treated as records.	

[18] Contact NARA for acceptable transfer formats. See 36 CFR 1228.270. Transfer formats are specified in records retention schedules.

Sample Test(s)	Expected Result(s)
Insert set of records and metadata to be destroyed. Issue destruction command for the records and metadata. Declare fact of destruction of records/metadata to be a record for each member of set.	Records of destructions are maintained. Records of destruction are not themselves capable of being destroyed.

1.5 Process Records Containing Restricted or National Security Classified Data

Criterion 1.5.1: The system captures National Security Classification metadata for classified records. These metadata elements include current classification, reason for (authority), classification source, derivative source (if any), declassification date, downgrade instructions, review date, reviewer, declassification date, and declassifier.

Sample Test(s)	Expected Result(s)
Import set of national security classified records to the system. Using an authorized user ID, enter metadata stipulating the records are classified for purposes of national security, and populate additional classification-related metadata elements.	Imported national security classified records are accepted successfully in system with associated metadata. Metadata stipulating classification status, plus additional related metadata, are successfully entered in the system.

Criterion 1.5.2: For derivatively classified records, the system supports the capability to capture multiple reasons ["Reason(s) for Classification"] and multiple sources ("Classified By") metadata elements.

Sample Test(s)	Expected Result(s)
Import or designate a set of derivatively classified records. Assign multiple reasons and multiples sources in the associated metadata for each record	Set of derivatively classified records is successfully designated or imported. Associated metadata for derivatively classified records successfully accepts multiple values for reasons and sources.

Criterion 1.5.3: The system provides a method for assigning classification levels to records (e.g., through a data or metadata field). The classification levels should include, but not be limited to: Confidential, Secret, Top Secret, and No Marking.

Sample Test(s)	Expected Result(s)
Enter five records and assign a different classification level to each record.	Each record includes in its metadata a Confidential, Secret, Top Secret, or No Marking classification.

Criterion 1.5.4: Authorized users can make changes to the retention period before declassification. [Note: Declassification review occurs outside the system.]

Sample Test(s)	Expected Result(s)
Use an authorized user ID to modify the retention period for a set of records.	For the designated set of records, the retention period is successfully modified.

1.6 Interface with RMA (Export Records)

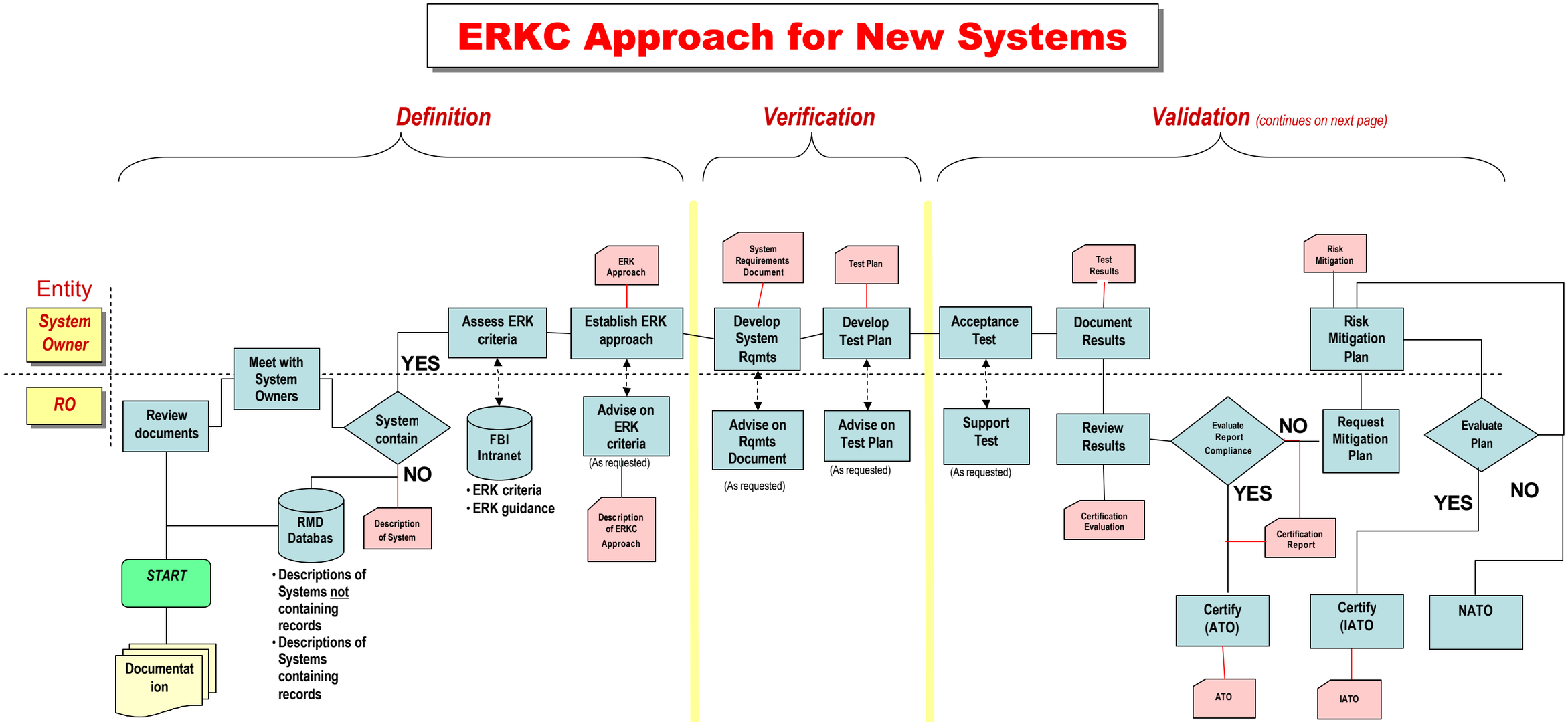
Criterion 1.6.1: The system exports records and history to the RMA.

Sample Test(s)	Expected Result(s)
Issue command to export a declared record and its history to the RMA.	Set of records and history are successfully received by the RMA. The system no longer contains the exported set of records and metadata.

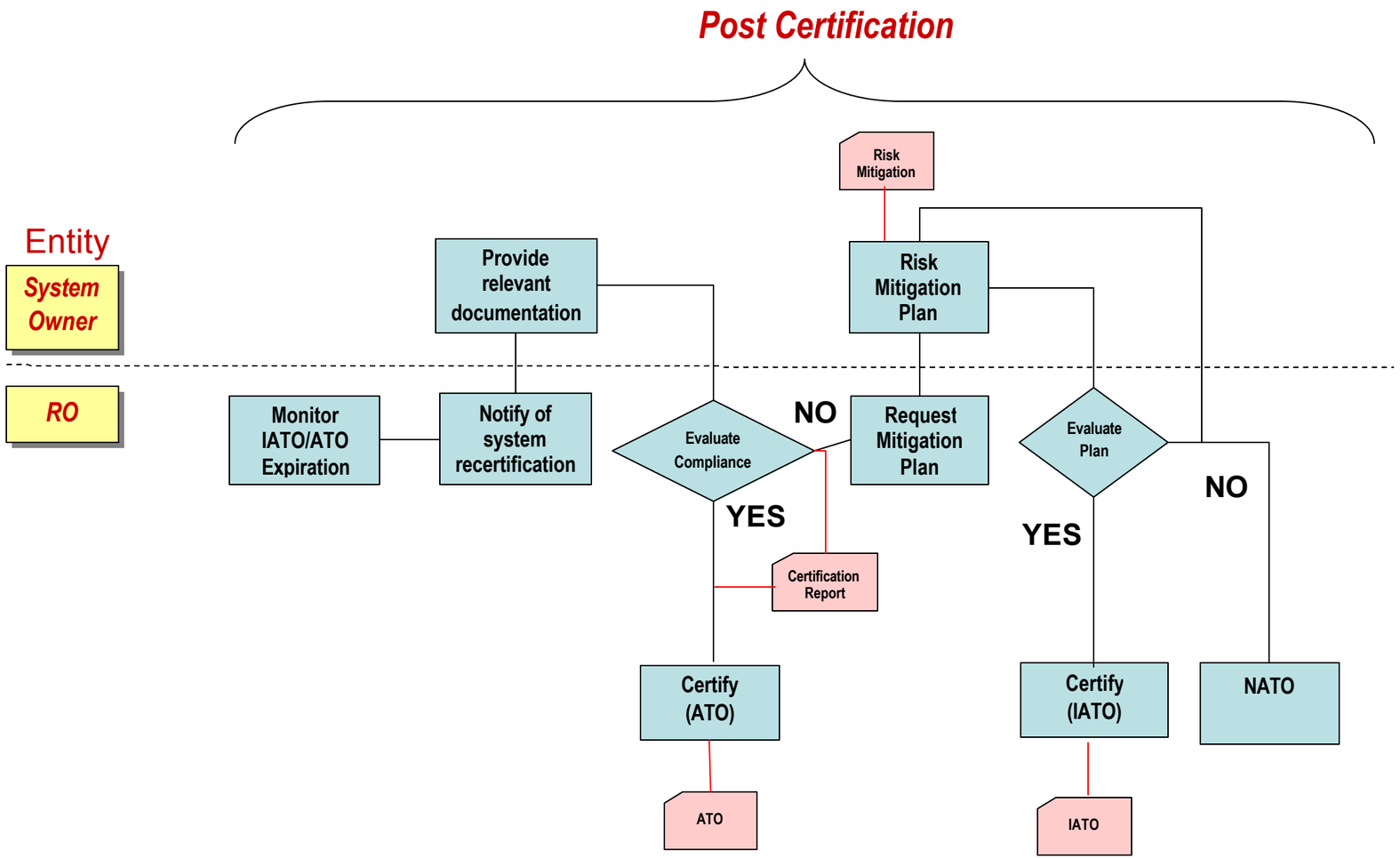
Criterion 1.6.2: The system exports metadata attached to records to the RMA.	
Sample Test(s)	**Expected Result(s)**
Issue command to export the metadata for a declared record to the RMA.	Set of metadata is successfully received by the RMA with the record. The system no longer contains the exported set of records and metadata.
Criterion 1.6.3: The system identifies and exports associated (linked) records and maintains record relationships.	
Sample Test(s)	**Expected Result(s)**
Select a test record that has associated records. Export the record to the RMA, indicating, if necessary, that you also want to transfer any associated records.	The known associated records are transferred to the RMA. The relationship between the records is maintained in the RMA.
Criterion 1.6.4: The system supports the capability to add needed metadata when records are exported.	
Sample Test(s)	**Expected Result(s)**
Access metadata of exported record from the sample test for Criterion 1.6.2 and fill in missing fields.	Metadata file is accessed. Metadata is successfully added.
Criterion 1.6.5: The system maintains pointers to exported records (i.e., associated records in the system should be linked to the exported record in the RMA). When a record is transferred from one system to another (the RMA), its "location" changes. Any pointers that pointed to the record in its "old location" need to be modified to reflect its "new location." For example, the system may contain past versions of a document (these versions may not be records, but documents), and the latest version is being transferred to a new RMA [possibly from a document management application (DMA)]. When a user opens up an outdated version of that document, the system should indicate that the latest version is located in the RMA.	
Sample Test(s)	**Expected Result(s)**
Issue command to export a record with associated records to the RMA.	Pointers in system will reflect the RMA identifier for the moved/exported record.
Criterion 1.6.6: Unique identifiers are transferred from source systems to the RMA (i.e., the system sends the unique identifier for a record from the original system to the RMA when a record is transferred to the RMA).	
Sample Test(s)	**Expected Result(s)**
Issue command to export a record from the system to the RMA. In the RMA, check the status of the field for the original identifier.	The original system's correct unique identifier is located in the metadata of the record in the RMA.

❖ ❖ ❖

Appendix D—ERKC Process Flow for New Systems

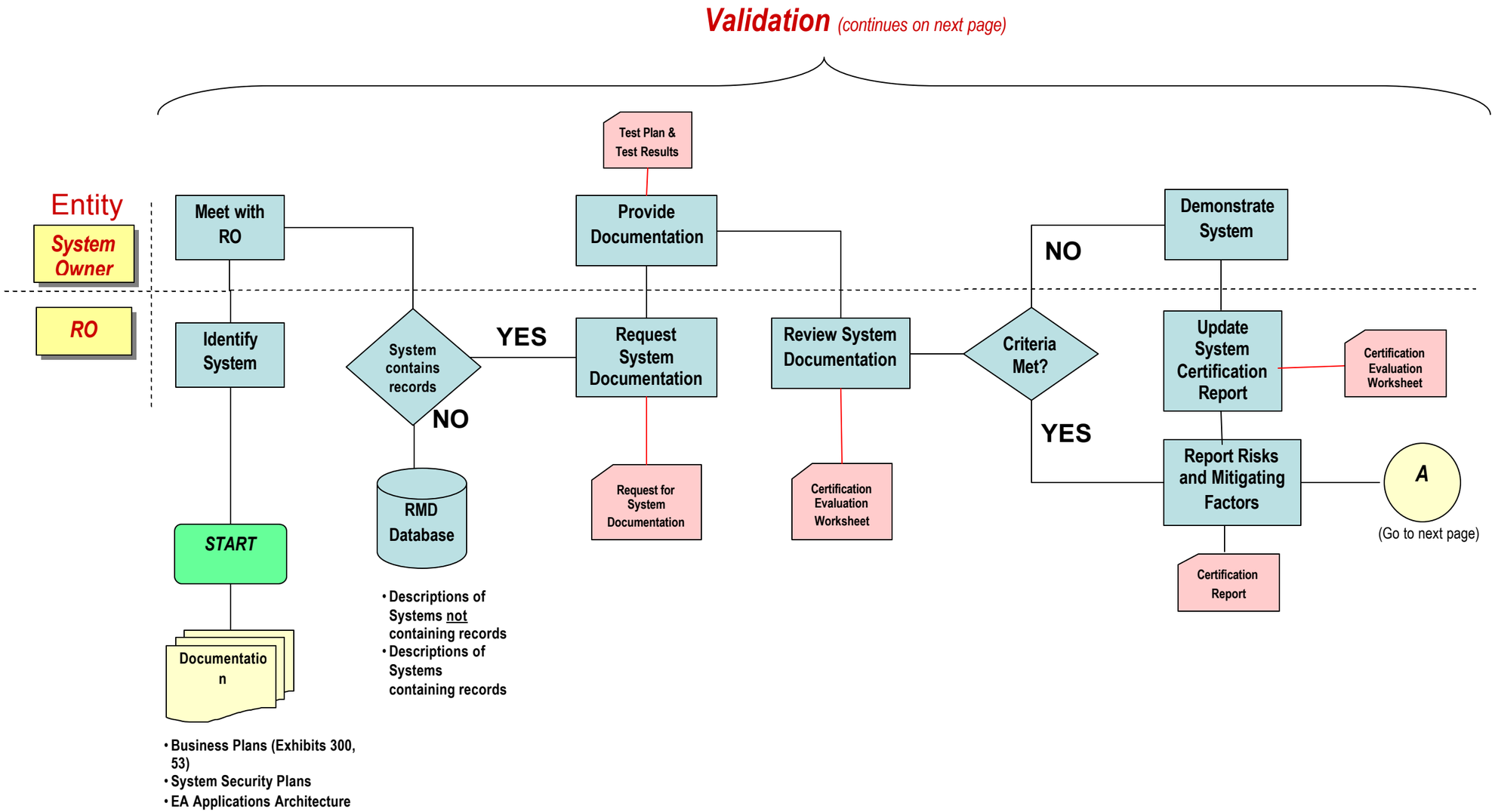


ERKC Approach for New Systems

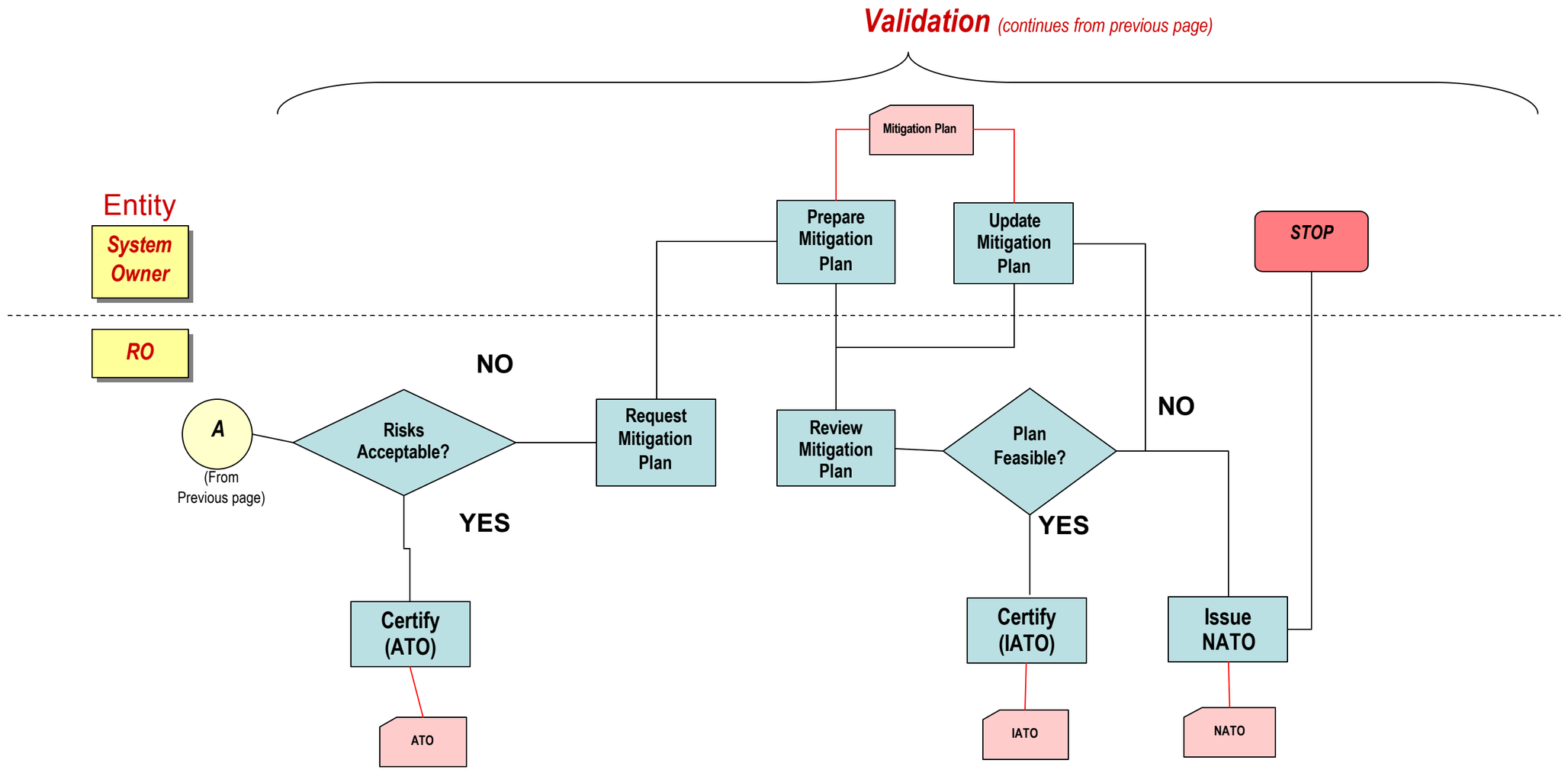


Appendix E—ERKC Process Flow for Legacy Systems

ERKC Approach for Legacy Systems



ERKC Approach for Legacy Systems



Appendix F—Risk Management

This appendix provides guidance on performing risk management in the context of determining vulnerabilities associated with the processing and use of electronic records. It is based on the electronic recordkeeping (ERK) criteria for FBI information systems (ISs) presented in Appendix C. The primary source of material for the information in Appendix F is NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, retrievable at http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

Risk Management provides a systematic process designed to identify and minimize the effects of risks and uncertainties. Risk management activities make risks visible and include assessing the probability of a risk's occurrence and its potential adverse effect. The potential adverse effect quantifies the magnitude of the loss to the effectiveness of Records Management in the FBI should the system be operated as an FBI IS.

Risk assessment is used to determine the extent of potential threats and risk associated with an IS throughout its system development life cycle (SDLC). The results of this process help to identify areas of concern—instances in which an FBI IS does not comply with ERK criteria—so the Records Officer (RO) can make a decision regarding system certification.

The electronic recordkeeping certification (ERKC) risk management process, described in the remainder of this appendix, is a guide for measuring potential ERK risk and reporting the level of that risk (i.e., its "seriousness") with respect to the ERK criteria for the system under consideration. The RO will use the results of an evaluation of risk (and any associated risk mitigation plans) in making the decision whether, and under what conditions, to certify an information system.

As noted above, the primary risk management activities are (1) risk analysis and (2) risk mitigation. Section F.1 describes the former and Section F.2 provides guidance on the latter.

F.1 Analyzing Risk

Figure F-1 provides an overview of the risk analysis process using the results of an evaluation of system compliance against ERK criteria. As noted in the figure, the process relies on the use of system documentation as its principal input. The process involves four primary activities, which are explained in the sections noted below:

- Tailor the ERK Compliance Evaluation Worksheet (Section F.1.1).
- Analyze system documentation (Section F.1.2).
- Determine the system risk scores (Section F.1.3).
- Determine the system risk level (Section F.1.4).

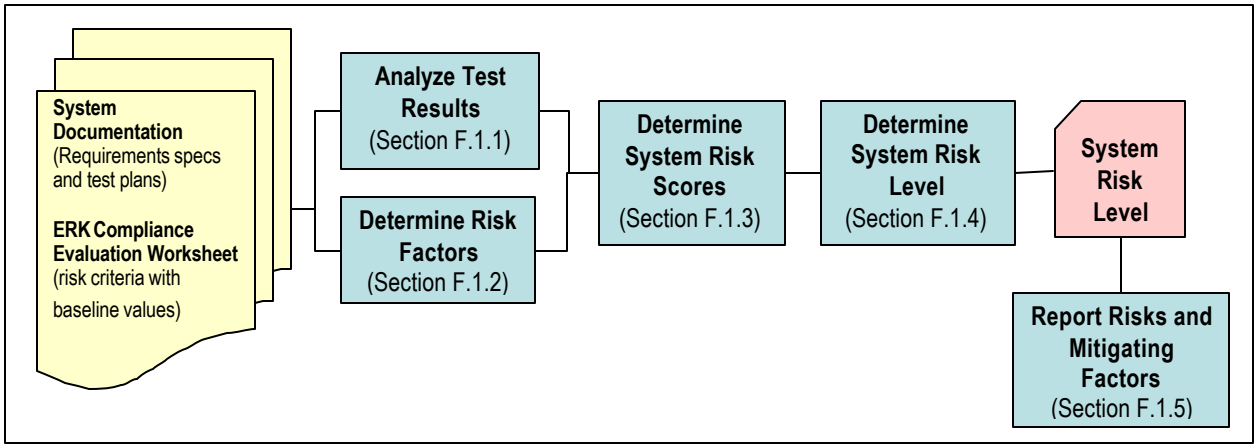


Figure F-1. ERKC Risk Analysis Process

F.1.1 Tailor ERK Compliance Evaluation Worksheet

The first step in the risk analysis process is for the Evaluator to determine, using the ERK Criteria Tailoring Tool, which criteria are applicable for evaluation. This determination is based upon the system's ERK "approach" and other system characteristics. The ERK Criteria Tailoring Tool is located in Appendix H. Section 1.4 provides information on the different architectural approaches to satisfying the ERK criteria.

In the ERK Compliance Evaluation Worksheet, located in Appendix I, the Evaluator directly assigns the Compliance Value to 1 for those criteria that are not applicable to the system, and makes a notation in the Comments column indicating the non-applicability of the criterion. Assigning a Compliance Value of 1 to non-applicable criteria ensures that systems are not described as being at higher risk should particular ERK criteria not apply.

Examples of other system characteristics that would make specific criteria not applicable (and therefore directly assigned a Compliance Value of 1 include the following:

- If the system under consideration does not contain Vital Records, the criterion relating to such records may have a Compliance Value of 1.
- If the system under consideration does not contain restricted or national security classified information, the criteria relating to such records may have a Compliance Value of 1.

In addition to the tailoring guidance provided by the ERK Criteria Tailoring tool, RMD is available to provide additional guidance on the assignment of Compliance Values.

F.1.2 Analyze System Documentation

In parallel with tailoring the ERK Compliance Evaluation Worksheet, the Evaluator analyzes the required system documentation developed in compliance with the FBI SDLC and examines it for evidence of functionality that satisfies the ERK Assessment Criteria. The Evaluator records the examination results in the ERK Compliance Evaluation Worksheet.

- If the evidence found in the documentation fully satisfies the ERK criterion, the ERKC Evaluator will assign a Compliance Value of 1, meaning the system satisfies this criterion 100 percent.
- If the evidence found in the documentation satisfies some percentage of the ERK criteria, the Compliance Value assigned is that percentage (expressed as a decimal between 0 and 1), which is multiplied by the Risk Baseline associated with the particular ERK risk criterion to calculate the Risk Score.
- As mentioned in Section F.1.1, if the risk criterion is not applicable to the system under consideration, the Compliance Value assigned is 1 – this ensures that systems are not described as being at higher risk should particular ERK criteria not apply. For example, certain ERK criteria are relevant only to those systems that contain classified information. Systems that do not contain classified information should not have a lower overall Risk Score (i.e. represent higher risk) because certain criteria are not applicable.

F.1.3 Determine System Risk Scores

For each criterion, compute the risk score by multiplying the Risk Baseline by the Compliance Value. In equation form, this can be expressed as:

$$\text{Risk Score} = \text{Risk Baseline} \times \text{Compliance Value}$$

For example, if a criterion's Risk Baseline is 5 and the compliance value is 0.5, (the Evaluator has determined that the system only half satisfies the criterion), the Risk Score would equal 2.5. If the Compliance Value is set to 1 – because the criterion does not apply to the system or the system fully satisfies the criteria – then the Risk Score will equal the Risk Baseline.

F.1.4 Determine System Risk Level

The final step in the process is to determine the overall system risk level. This step involves computing the overall Risk Score and analyzing the results. Such an analysis must include examination of the potential implications of a system not meeting certain ERK criteria, consideration of mitigating factors, as well as an examination of the risks aggregated into their risk classes (Declare Records, Capture Records, etc.).

To compute the overall risk score, sum the individual risk scores for all criteria (including those that were deemed not applicable to the system). Because there are complementary risks within classes, the class-level risk must also be calculated. It is important to note that the lower the risk score, the higher the overall risk.

An important aspect of the risk analysis is to determine the potential implications associated with any criteria for which less-than-complete satisfaction was demonstrated by the test results (i.e., those criteria for which the compliance value is less than one). The System Owner must use his or her judgment (perhaps working in cooperation with the RMD) to develop these potential implications. The Comment column in the ERK Compliance Evaluation Worksheet may be used to record the implications. This information will serve as the foundation for any mitigation plan to be developed by the System Owner to obtain an Interim Authority to Operate (IATO) - see Sections 2.2.3 and 2.3.1, respectively, for information on risk mitigation plans for new and legacy systems.

F.1.5 Report Risks and Mitigating Factors

Using the completed ERK Compliance Evaluation Worksheet and notes from meetings with the System Owner, the ERKC Evaluator develops the ERK System Certification Report. The report summarizes the results of the system evaluation and should focus on descriptions of risks and unique system characteristics that either mitigate or exacerbate risk. The report is organized by the 11 criteria classes (Declare Records, Capture Records, etc.) to ensure that related risks are discussed together to provide sufficient context to support a certification decision by the RO. A template of this report is located in Appendix J. The final ERK System Certification Report consists of this risk analysis supported by the final completed ERK Compliance Evaluation Worksheet.

F.2 Mitigating Risk

Each risk identified as a result of the risk analysis process should have a mitigation strategy. (This is mandatory if the RO requires a System Owner to prepare a risk mitigation plan.) Risk mitigation is the analysis of trade-offs among alternative sets of possible safeguards. A mitigation countermeasure is the method that will be taken to lessen or alleviate the adverse effect of the risk. For ERKC, the ultimate recommended countermeasure would be the selection and implementation of one of the approved ERK approaches (see section 1.4 for definitions of these approaches). However, interim countermeasures may also be effective in reducing the system risk level.

Examples of possible mitigation strategies include:

- Using an alternative method of storing records (e.g., printing out and filing records in paper form) until the ability to transfer records to the FBI RMA is built into the system.
- Including the desired feature in the next version of the system that is funded for the following year.
- Determining that the system is a temporary one and will outlive its usefulness (or be replaced) within the following year.

Using the information in the ERK Compliance Evaluation Worksheet, the System Owner should create a risk mitigation plan (also called an action plan). One method would be to extract the criterion number and the potential implication and put them in the ERK Risk Mitigation Worksheet shown below. The System Owner may then document the mitigation countermeasures or recommended countermeasures in the worksheet. Implications and countermeasures should have a one-to-one relationship. The Risk Mitigation Worksheet provides the core content of a risk mitigation plan, should the latter be required by the RO.

ERK Risk Mitigation Worksheet		
Criterion Number	**Potential Implication**	**Mitigation / Recommended Countermeasures**

Appendix G—System Evaluation Process Details

This appendix provides detailed instructions for evaluating how well the system under consideration complies with the electronic recordkeeping (ERK) Assessment Criteria.

The Validation phase of the electronic recordkeeping certification (ERKC) process is designed to identify how well the system satisfies the ERK criteria. It is designed to take advantage of existing system documentation to avoid duplication of effort and placing additional unnecessary burden on the System Owner. Figure G-1 depicts an overview of this process and describes how the various tools, worksheets, and criteria contained in the appendices of this manual are used together to evaluate information systems for compliance with ERK criteria.

The primary inputs to this process are:

- ERK Assessment Criteria (Appendix C)
- ERK Criteria Tailoring Tool (Appendix H)
- System documentation
- ERK Compliance Evaluation Worksheet (Appendix I)
- List of RMA Metadata (Appendix M)

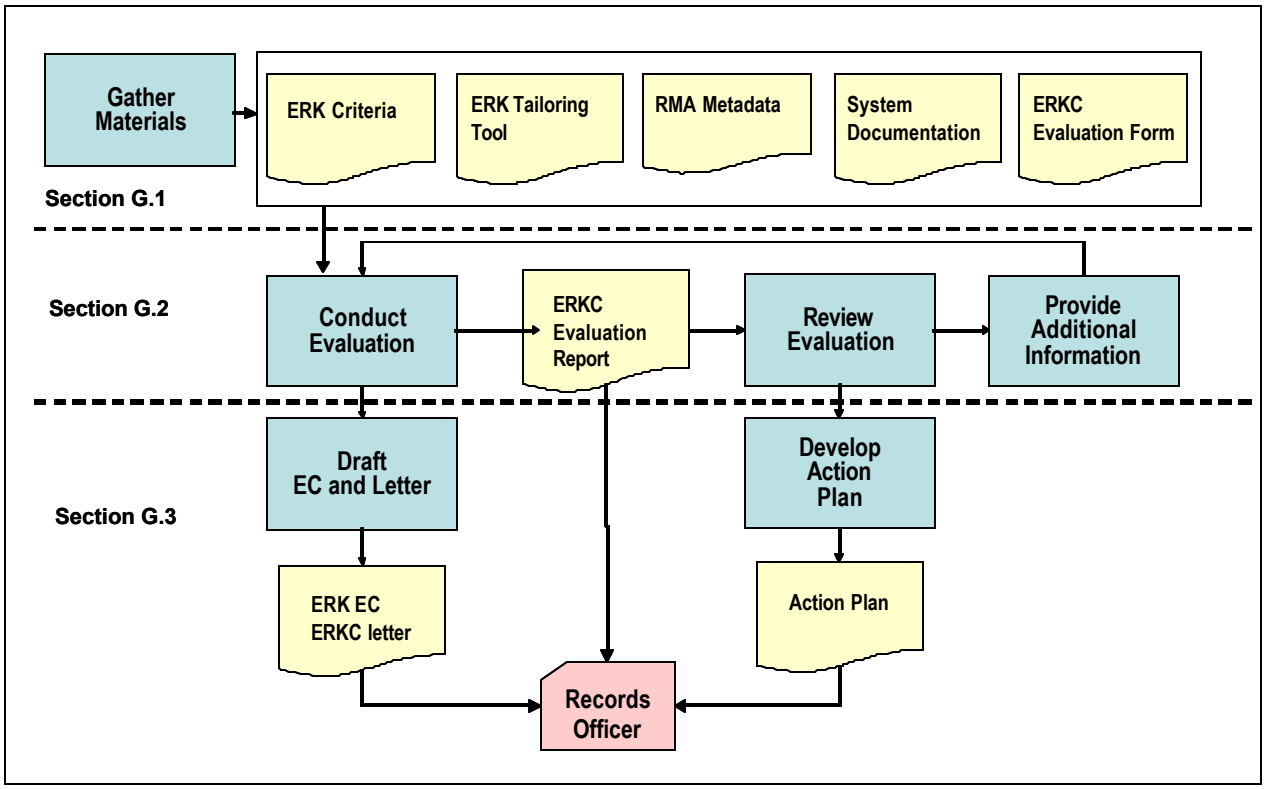


Figure G-1. ERKC Validation Phase Process

G.1 Prepare for the Validation Phase

The Evaluator assembles the materials. The system documentation is provided by the System Owner. The ERK Assessment Criteria, the ERK Criteria Tailoring Tool, ERK Compliance Evaluation Worksheet, and List of RMA Metadata are included as appendices to this Manual and will be available on the RMD Web site.

The most useful system documentation to support the validation phase process is the test results from a system functional test and a Security Certification and Accreditation (C&A) test. If these are not available, the system requirements would be most useful, after which would be system design documents or user's manual.

With knowledge of the ERK approach of the system (i.e., Integration, Direct Export, or Integral), the ERK Criteria Tailoring Tool is used to tailor the criteria to those required by the system. Following the instructions for the tool, a Compliance Value of 1 can be entered on the ERK Compliance Evaluation Worksheet (as described in Section F.1.1) for non-applicable criteria prior to any detailed examination of the system documentation.

G.2 Evaluate System Compliance

As shown in Figure G-1, the evaluation process mainly consists of an interaction, or series of interactions, between the ERK Evaluator and the System Owner. Proper evaluation cannot be conducted without an understanding of the context of the subject application, as well as the role of the system in the business.

Initially, the Evaluator follows the steps in the risk analysis process described in section F.1.2, matching the documentation with the ERK Assessment Criteria and using its tests and expected results as aids to determine what criteria are met according to the system documentation. The List of RMA Metadata, which includes all required FBI RMA metadata elements, is used in evaluating the criteria that address metadata. The list is presented in Appendix M.

The Evaluator uses the evaluation worksheet to document the results of the evaluation, making notes in the Comment column for any criterion that does not appear to be satisfied, or for which questions remain. The Adverse Effect column can be modified to include specific adverse effects from the unmet criteria.

After the evaluation of the system documentation is documented in a draft ERK Compliance Evaluation Worksheet, the Evaluator meets with the System Owner to review the results. The goal of this meeting is not to defend preliminary assessments, but to develop a common understanding of both the system and the ERK criteria. During this meeting, adjustments to the Compliance Values are encouraged as the ERK Evaluator gains further insight into the system. As much of the success of this process depends on System Owners understanding the ERK criteria so that they can develop appropriate requirements specifications that will lead eventually to full compliance, the ERK Evaluator must strive to promote understanding and help the System Owner identify ways to satisfy ERKC requirements. Oftentimes, for example, systems support

business processes result in records, but systems owners may not be aware that a final approval that results in the publishing of a document, or Web page, may constitute the declaration of a record, and that only minor changes may be required to fully comply with relevant records declaration criteria.

System Owners should be encouraged to provide additional documentation as evidence of compliance with ERK criteria. Oftentimes, for example, systems maintain audit information that is not documented in either requirements specifications or test plans as end-users rarely have use for such information. Sample audit reports are excellent evidence of compliance with audit related criteria. Responsibilities for training to help the System Owner understand how to treat audit data as records, however, should be assumed by the ERK Evaluator.

G.3 Document the Evaluation

Using the completed ERK Compliance Evaluation Worksheet and notes from meetings with the System Owner, the ERKC Evaluator develops the ERK System Certification Report. The report summarizes the results of the system evaluation and should focus on descriptions of risks and unique system characteristics that either mitigate or exacerbate risk. The Worksheet should be included as an appendix to the Report.

When the System Owner and Evaluator agree that the ERK System Certification Report accurately represents the situation, the System Owner develops a risk mitigation plan (also known as an action plan) for the unmet ERK criteria, as discussed in section F.2.

The Evaluator drafts the ERK Certification Letter and the ERKC Electronic Communication (EC). The purpose of the Letter is to certify the system and delineate the terms of the certification. The purpose of the ERKC EC is to notify the System Owner of the certification. A sample Letter and EC are included Appendices K and L, respectively, and will be available on the RMD Web site.

The outputs from the process are:

- Completed ERK System Certification Report, including the ERK Compliance Evaluation Worksheet as an appendix (Appendix J)
- System Risk Mitigation Plan (if needed)
- Draft ERK Certification Letter (Appendix K)
- Draft ERK Electronic Communication (Appendix L)

The outputs from this process are sent to the Records Officer as input for the decision whether or not to authorize the operation of the system.

Appendix H—ERK Criteria Tailoring Tool

The ERK Criteria Tailoring Tool is used to determine which ERK criteria are to be included in the system according to the ERK approach determined by the System Owner or project manager.

Find the column in the table that correlates to the ERK approach of the system. Those criteria marked with an "X" in that column should be included in the system's design to ensure compliance with the FBI electronic recordkeeping certification process.

Criterion	Integration With RMA	Direct Export	Integral
1.1 DECLARE RECORDS (Allow information to be designated as a record)			
1.1.1 The system designates specified information as records, either manually or automatically.	X		X
1.1.2 The system assigns unique identifiers to records and their associated metadata. The system prevents any modification of a record's unique identifier, once it is defined.	X	X	X
1.1.3 The system captures record metadata (FBI-designated and others) automatically and reliably links metadata to the records.	X		X
1.2 CAPTURE RECORDS			
1.2.1 The system imports records from sources outside the system (e.g., other information systems, desktop applications, scanned documents, or e-mail) along with all required associated metadata (e.g., records series, pre-existing file plans, or locations for physical records)	X		X
1.2.2 To provide records management control over the records without physically transporting them to an RMA, the system links records to an external RMA.	X	X	X
1.3 MAINTAIN OR USE RECORDS			
1.3.1 RECORDS ORGANIZATION			
1.3.1.1 The system accepts an FBI-specific scheme for organizing records. For example, the system accepts FBI-specific records retention schedules and organizes records according to the schedules.		X	X
1.3.1.2 Users can select categories in which records are filed and assign records to these categories.		X	X

Criterion	Integration With RMA	Direct Export	Integral
1.3.1.3 The system supports assignment of Vital Record indicators.	X		X
1.3.1.4 The system supports linking of related records (e.g., a redacted record with its non-redacted counterpart, an original record with its revision, or an electronic record with a paper antecedent).		X	X
1.3.1.5 The system supports the capability for users to create and edit file plans, including categories and sub-categories. The system prevents deletion of non-empty folders.		X	X
1.3.1.6 The system can assign a status to records to prevent destruction (i.e., the system contains an indicator that includes an option to mark records as "do-not-destroy," which prevents records from being selected for destruction or transfer according to records retention schedules).		X	X
1.3.1.7 The system supports global changes to metadata, file plans, and records retention schedules.			X
1.3.1.8 The system executes disposition instructions (e.g., moves a group of records from active to inactive status or designates a group of records for destruction or transfer).			X
1.3.1.9 For systems that manage physical records, the system specifies identifiers for boxes, contents, locations, etc. In other words, the system stores metadata for records not contained in the system and can identify records by physical location (box number, location ID, etc.)			X
1.3.2 RECORDS SECURITY			
1.3.2.1 The system prevents over-writing records. To comply with records management guidelines, records are never edited, but new versions are created and linked to the source.	X	X	X
1.3.2.2 The system prevents deletion of indices, categories, and other 'pointers' to records (i.e., maintains referential integrity).	X	X	X
1.3.2.3 The system provides an automatic method to detect any alteration of records or metadata.		X	X

Criterion	Integration With RMA	Direct Export	Integral
1.3.2.4 The system provides audit trails of all add, update, deletion, and retrieval activity.	X	X	X
1.3.2.5 The system (or System Owner) maintains appropriate backup copies of records and recordkeeping systems.	X	X	X
1.3.2.6 The system is protected by adequate recovery/rollback and rebuild procedures so that records may be recovered or restored following a system malfunction.	X	X	X
1.3.3 RECORDS ACCESS			
1.3.3.1 The system controls access so that only authorized individuals are able to retrieve, view, print, copy, or edit records or other entities (e.g., metadata, file plan, etc.) in the recordkeeping system.			X
1.3.3.2 The system identifies individuals and groups of users and allows different access privileges to be assigned to individuals or groups.		X	X
1.3.3.3 The system maintains the integrity of redacted records and assures that redacted material is not accessible on sealed records.	X	X	X
1.3.4 RECORDS RETRIEVAL			
1.3.4.1 The system ensures that all access privileges (permissions and restrictions) are enforced on all retrievals.			X
1.3.4.2 The system can retrieve records and their associated metadata and can retrieve records based on defined links (e.g., between versions of the same record or between the records in a particular case file).			X
1.3.4.3 The system provides a sufficiently powerful range of search features and options, as needed to meet agency requirements. These might include: searching on individual terms or a combination of terms, wildcard or exact-match searching, proximity or adjacency searching, relevance ranking of search results, use of stop words, limits on maximum size of results set from a search, query by image content, or others.			X

Criterion	Integration With RMA	Direct Export	Integral
1.3.5 RECORDS PRESERVATION			
1.3.5.1 The system provides users the capability to read and accurately interpret all records (and metadata) in the system throughout their useful life. The system has capability to continuously sample older records for the ability to machine-read records and their metadata, and reports failures to machine-read.			X
1.3.5.2 The system enables migration of records and metadata to new storage media or formats in a way that the content is retained and understandable in order to avoid loss due to media decay or technology obsolescence.			X
1.3.5.3 The system ensures that captured metadata remains linked to appropriate records without alteration throughout the useful life of the records. The system supports the capability to continuously sample records to verify that metadata remain associated with records and to output results of the sampling process.			X
1.3.6 AUDIT/OVERSIGHT			
1.3.6.1 The system provides access to summary reports (e.g., number of accesses) and detail level audit trail information (e.g., each individual record access, including record identifier, date, time and user). The system supports the capability to continuously compile and output periodic and on-demand reports of summary and detailed audit trail information.			X
1.3.6.2 The system tracks failed attempts of all records activity and system functions. In other words, the system detects, records and outputs any unsuccessful attempts to access records or metadata, or conduct other system functions. The system tracks information such as user ID, date and time of failed attempts.			X
1.3.6.3 Audit trail information is managed as records in order to prevent editing of audit logs.		X	X

Criterion	Integration With RMA	Direct Export	Integral
1.4 DISPOSE OF RECORDS (FINAL) (Transfer or destroy)			
1.4.1 The system identifies records eligible for transfer or destruction based on records retention schedules and disposition instructions (i.e., the system automatically detects when a record's retention period will pass, notifies the Records Officer that the record is eligible for disposition, and stipulates whether the record is eligible for transfer or destruction).			X
1.4.2 The system exports records and metadata to be transferred (i.e., copy and subsequently remove them from the system) in a format acceptable for transfer to NARA.			X
1.4.3 The system deletes records to be destroyed so they cannot be physically reconstructed or otherwise retrie ved.	X	X	X
1.4.4 The system maintains a record of all record transfers and destructions and provides certifiable proof of transfer or destruction. All records of transfer or destruction are treated as records.			X
1.5 PROCESS RECORDS CONTAINING RESTRICTED OR NATIONAL SECURITY CLASSIFIED DATA (ERK systems maintaining restricted or national security classified data shall:)			
1.5.1 The system captures National Security Classification metadata for classified records. These metadata elements include current classification, reason for (authority), classification source, derivative source (if any), declassification date, downgrade instructions, review date, reviewer, declassification date, and declassifier.	X	X	X
1.5.2 For derivatively classified records, the system supports the capability to capture multiple reasons ["Reason(s) for Classification"] and multiple sources ("Classified By") metadata elements.		X	X
1.5.3 The system provides a method for assigning classification levels to records (e.g., through a data or metadata field). The classification levels should include, but not be limited to: Confidential, Secret, Top Secret, and No Marking.	X	X	X
1.5.4 Authorized users can make changes to the retention period before declassification. [Note: Declassification review occurs outside the system.]			X

Criterion	Integration With RMA	Direct Export	Integral
1.6 INTERFACE WITH RMA (EXPORT RECORDS) (ERK systems that export records to an RMA shall:)			
1.6.1 The system exports records and history to the RMA.		X	
1.6.2 The system exports metadata attached to records to the RMA.		X	
1.6.3 The system identifies and exports associated (linked) records and maintains record relationships.		X	
1.6.4 The system supports the capability to add needed metadata when records are exported.		X	
1.6.5 The system maintains pointers to exported records (i.e., associated records in the system should be linked to the exported record in the RMA). When a record is transferred from one system to another (the RMA), its "location" changes. Any pointers that pointed to the record in its "old location" need to be modified to reflect its "new location." For example, the system may contain past versions of a document (these versions may not be records, but documents), and the latest version is being transferred to a new RMA [possibly from a document management application (DMA)]. When a user opens up an outdated version of that document, the system should indicate that the latest version is located in the RMA.		X	
1.6.6 Unique identifiers are transferred from source systems to the RMA (i.e., the system sends the unique identifier for a record from the original system to the RMA when a record is transferred to the RMA).		X	

Appendix I—ERK Compliance Evaluation Worksheet

Electronic Recordkeeping (ERK) Compliance Evaluation Worksheet

[System Name]

Prepared by Electronic Records Section Staff

[Team Lead], Test Team Leader

Reviewed by [Reviewer's Name]

Submitted on [Date]

The ERK Compliance Evaluation Worksheet consists of a table that lists each of the ERK Assessment Criteria and provides space in the table columns to indicate the system's compliance with each criterion and the implications of non-compliance or partial compliance with particular criteria. The worksheet is completed during the Analyzing Risk Phase (Section F.1) of the ERKC process.

The Risk Baseline is a pre-filled column that contains the baseline value for each criterion. Baseline values are rated from 0 to 5; the more critical the criterion, the higher the baseline value. Baseline values provide a starting point for determining the level of the risk incurred by non-compliance or partial-compliance with the criterion, which is determined by evaluating how well the test results and other system documentation reflect "satisfaction" against each criterion.

The Compliance Value column should be filled out by the Evaluator. The Compliance Value is rated on a scale of 0 to 1; a Compliance Value of 1 indicates complete compliance with the criterion and a Compliance Value of 0 indicates total non-compliance. If the criterion is half satisfied, the Compliance Value for that criterion would be 0.5.

The Risk Score column should also be completed by the Evaluator. The Risk Score is equal to the Risk Baseline multiplied by the Compliance Value. For example, if the Risk Baseline for a particular criterion is 5, and the Compliance Value is 0.5, then the Risk Score equals 2.5, or $5 \times 0.5 = 2.5$.

The Adverse Effect is a pre-filled column that describes the potential adverse effect if the criterion is not satisfied. However, the contents of an individual cell may be modified to suit the particular system under evaluation.

The Comment column is a space for the Evaluator to note information such as aspects of the system related to the criterion or class, and observances made during the risk analysis.

The ERK Criteria Tailoring Tool, described in Section F.1.1 and located in Appendix H, is used to determine which ERK criteria below are applicable to the specific system. The tool consists of a table that lists each of the ERK Assessment Criteria and includes columns for each ERK approach (i.e., Integration with RMA, Direct Export, or Integral). The Evaluator determines the column that corresponds to the ERK approach of the system. Those criteria marked with an "X" in that column should be included in the system's design to ensure compliance with the FBI electronic recordkeeping certification process. All other criteria are not applicable to the system under consideration and are not required for ERK certification of the system. In the ERK Compliance Evaluation Worksheet below, the Compliance Value assigned to these non-applicable criteria is 1. Doing this ensures that the system does not have a lower overall risk score (i.e. represent higher risk) should particular ERK criteria not apply.

The ERK Compliance Evaluation Worksheet should be included as an appendix to the ERK System Certification Report, a template of which is located in Appendix J, and together they will be used by the Records Officer to make an ERK certification decision and determine the level of certification the system will receive.

	System:	**<system name>**	
Test Team Lead		Reviewer	
Test Team Member			

Revision History			
Revision Number	**Date**	**Author(s)**	**Description of Changes**
			Draft
			Draft with Corrections
			Final Submitted Version

Criterion	Risk Baseline	Compliance Value	Risk Score	Adverse Effect	Comment
1.1 DECLARE RECORDS (Allow information to be designated as a record)					
1.1.1 The system designates specified information as records, either manually or automatically.	**5**			Cannot link retention information unless identified as record.	
1.1.2 The system assigns unique identifiers to records and their associated metadata. The system prevents any modification of a record's unique identifier, once it is defined.	**5**			Need unique identifier to differentiate between similar records.	
1.1.3 The system captures record metadata (FBI-designated and others) automatically and reliably links metadata to the records.	**4**			Metadata not automatically entered must be entered manually.	

Criterion	Risk Baseline	Compliance Value	Risk Score	Adverse Effect	Comment
Class Summary	***14***				
1.2 CAPTURE RECORDS					
1.2.1 The system imports records from sources outside the system (e.g., other information systems, desktop applications, scanned documents, or e-mail) along with all required associated metadata (e.g., records series, pre-existing file plans, or locations for physical records).	**3**			Cannot import records.	
1.2.2 To provide records management control over the records without physically transporting them to an RMA, the system links records to an external RMA.	**3**			Cannot link to an RMA.	
Class Summary	***6***			*If the system cannot capture records, it is limited in the records that it can contain.*	
1.3 MAINTAIN OR USE RECORDS					
1.3.1 RECORDS ORGANIZATION					
1.3.1.1 The system accepts an FBI-specific scheme for organizing records. For example, the system accepts FBI-specific records retention schedules and organizes records according to the schedules.	**5**			Do not have basis for retention and disposition.	
1.3.1.2 Users can select categories in which records are filed and assign records to these categories.	**4**			Cannot assign retention and disposition.	

Criterion	Risk Baseline	Compliance Value	Risk Score	Adverse Effect	Comment
1.3.1.3 The system supports assignment of Vital Record indicators.	**3**			Cannot automatically identify vital records contained in system.	
1.3.1.4 The system supports linking of related records (e.g., a redacted record with its non-redacted counterpart, an original record with its revision, or an electronic record with a paper antecedent).	**3**			If related records are not linked, it is harder to identify all related records. Run risk of working off wrong version.	
1.3.1.5 The system supports the capability for users to create and edit file plans, including categories and sub-categories. The system prevents deletion of non-empty folders.	**4**			Not limiting actions to authorized users can cause chaos and undermine the schedule.	
1.3.1.6 The system can assign a status to records to prevent destruction (i.e., the system contains an indicator that includes an option to mark records as "do-not-destroy," which prevents records from being selected for destruction or transfer according to records retention schedules).	**4**			Legal ramifications for deleting records that should have had action suspended.	
1.3.1.7 The system supports global changes to metadata, file plans, and records retention schedules.	**2**			Use of more staff time to make individual changes manually.	
1.3.1.8 The system executes disposition instructions (e.g., moves a group of records from active to inactive status or designates a group of records for destruction or transfer).	**4**			Manual searching for records that are ready for disposition.	

Criterion	Risk Baseline	Compliance Value	Risk Score	Adverse Effect	Comment
1.3.1.9 For systems that manage physical records, the system specifies identifiers for boxes, contents, locations, etc. In other words, the system stores metadata for records not contained in the system and can identify records by physical location (box number, location ID, etc.)	**2**			Related physical and electronic records are not connected, could be "lost."	
Class Summary	***30***				
1.3.2 RECORDS SECURITY					
1.3.2.1 The system prevents over-writing records. To comply with records management guidelines, records are never edited, but new versions are created and linked to the source.	**5**			Degradation of reliability of record keeping practices.	
1.3.2.2 The system prevents deletion of indices, categories, and other 'pointers' to records (i.e., maintains referential integrity).	**4**			Degradation of reliability of record keeping practices.	
1.3.2.3 The system provides an automatic method to detect any alteration of records or metadata.	**4**			Degradation of reliability of record keeping practices.	
1.3.2.4 The system provides audit trails of all add, update, deletion, and retrieval activity.	**3**			Degradation of reliability of record keeping practices.	
1.3.2.5 The system (or System Owner) maintains appropriate backup copies of records and recordkeeping systems.	**3**			Loss of records if system malfunctions, power is lost, etc.	

Criterion	Risk Baseline	Compliance Value	Risk Score	Adverse Effect	Comment
1.3.2.6 The system is protected by adequate recovery/rollback and rebuild procedures so that records may be recovered or restored following a system malfunction.	**3**			Loss of records if system malfunctions, power is lost, etc.	
Class Summary	***22***				
1.3.3 RECORDS ACCESS					
1.3.3.1 The system controls access so that only authorized individuals are able to retrieve, view, print, copy, or edit records or other entities (e.g., metadata, file plan, etc.) in the recordkeeping system.	**4**			Degradation of reliability of record keeping practices.	
1.3.3.2 The system identifies individuals and groups of users and allows different access privileges to be assigned to individuals or groups.	**4**			Degradation of reliability of record keeping practices.	
1.3.3.3 The system maintains the integrity of redacted records and assures that redacted material is not accessible on sealed records.	**3**			Release of unauthorized or personal information.	
Class Summary	***11***				
1.3.4 RECORDS RETRIEVAL					
1.3.4.1 The system ensures that all access privileges (permissions and restrictions) are enforced on all retrievals.	**4**			Degradation of reliability of record keeping practices.	

Criterion	Risk Baseline	Compliance Value	Risk Score	Adverse Effect	Comment
1.3.4.2 The system can retrieve records and their associated metadata and can retrieve records based on defined links (e.g., between versions of the same record or between the records in a particular case file).	**3**			Breakdown of links between records and metadata or related records require more staff time to find records.	
1.3.4.3 The system provides a sufficiently powerful range of search features and options, as needed to meet agency requirements. These might include: searching on individual terms or a combination of terms, wildcard or exact-match searching, proximity or adjacency searching, relevance ranking of search results, use of stop words, limits on maximum size of results set from a search, query by image content, or others.	**3**			If search capabilities are not robust enough, more staff time is spent finding the correct records.	
Class Summary	***10***				
1.3.5 RECORDS PRESERVATION					
1.3.5.1 The system provides users the capability to read and accurately interpret all records (and metadata) in the system throughout their useful life. The system has capability to continuously sample older records for the ability to machine-read records and their metadata, and reports failures to machine-read.	**5**			Cannot use records.	

Criterion	Risk Baseline	Compliance Value	Risk Score	Adverse Effect	Comment
1.3.5.2 The system enables migration of records and metadata to new storage media or formats in a way that the content is retained and understandable in order to avoid loss due to media decay or technology obsolescence.	**4**			Maintenance of outdated technology for life of records.	
1.3.5.3 The system ensures that captured metadata remains linked to appropriate records without alteration throughout the useful life of the records. The system supports the capability to continuously sample records to verify that metadata remain associated with records and to output results of the sampling process.	**4**			Lose of record integrity.	
Class Summary	***13***				
1.3.6 AUDIT/OVERSIGHT					
1.3.6.1 The system provides access to summary reports (e.g., number of accesses) and detail level audit trail information (e.g., each individual record access, including record identifier, date, time and user). The system supports the capability to continuously compile and output periodic and on-demand reports of summary and detailed audit trail information.	**3**			Staff time to get same information manually.	

Criterion	Risk Baseline	Compliance Value	Risk Score	Adverse Effect	Comment
1.3.6.2 The system tracks failed attempts of all records activity and system functions. In other words, the system detects, records and outputs any unsuccessful attempts to access records or metadata, or conduct other system functions. The system tracks information such as user ID, date and time of failed attempts.	**4**			Loss of audit reliability.	
1.3.6.3 Audit trail information is managed as records in order to prevent editing of audit logs.	**4**			Loss of audit reliability.	
Class Summary	***11***				
1.4 DISPOSE OF RECORDS (FINAL) (Transfer or destroy)					
1.4.1 The system identifies records eligible for transfer or destruction based on records retention schedules and disposition instructions (i.e., the system automatically detects when a record's retention period will pass, notifies the Records Officer that the record is eligible for disposition, and stipulates whether the record is eligible for transfer or destruction).	**5**			Staff time needed to identify eligible records.	
1.4.2 The system exports records and metadata to be transferred (i.e., copy and subsequently remove them from the system) in a format acceptable for transfer to NARA.	**4**			Staff time needed to extract and/or reformat records.	
1.4.3 The system deletes records to be destroyed so they cannot be physically reconstructed or otherwise retrieved.	**5**			Degradation of reliability of record keeping practices.	

Criterion	Risk Baseline	Compliance Value	Risk Score	Adverse Effect	Comment
1.4.4 The system maintains a record of all record transfers and destructions and provides certifiable proof of transfer or destruction. All records of transfer or destruction are treated as records.	**4**			Staff time to create and maintain record of transfers and destructions.	
Class Summary	***18***				
1.5 PROCESS RECORDS CONTAINING RESTRICTED OR NATIONAL SECURITY CLASSIFIED DATA					
1.5.1 The system captures National Security Classification metadata for classified records. These metadata elements include current classification, reason for (authority), classification source, derivative source (if any), declassification date, downgrade instructions, review date, reviewer, declassification date, and declassifier.	**5**			Loss of pertinent information.	
1.5.2 For derivatively classified records, the system supports the capability to capture multiple reasons ["Reason(s) for Classification"] and multiple sources ("Classified By") metadata elements.	**4**			Loss of pertinent information.	
1.5.3 The system provides a method for assigning classification levels to records (e.g., through a data or metadata field). The classification levels should include, but not be limited to: Confidential, Secret, Top Secret, and No Marking.	**4**			Loss of control on classified material.	
1.5.4 Authorized users can make changes to the retention period before declassification. [Note: Declassification review occurs outside the system.]	**3**			Loss of control on classified material.	
Class Summary	***16***				

Criterion	Risk Baseline	Compliance Value	Risk Score	Adverse Effect	Comment
1.6 INTERFACE WITH RMA (EXPORT RECORDS)					
1.6.1 The system exports records and history to the RMA.	**5**			Degradation of reliability of record keeping practices.	
1.6.2 The system exports metadata attached to records to the RMA.	**4**			Staff time to research data and manually add it to RMA.	
1.6.3 The system identifies and exports associated (linked) records and maintains record relationships.	**4**			Staff time to manually identify associated records, potential incomplete	
1.6.4 The system supports the capability to add needed metadata when records are exported.	**5**			Staff time to research data and manually add it to RMA.	
1.6.5 The system maintains pointers to exported records (i.e., associated records in the system should be linked to the exported record in the RMA). When a record is transferred from one system to another (the RMA), its "location" changes. Any pointers that pointed to the record in its "old location" need to be modified to reflect its "new location." For example, the system may contain past versions of a document (these versions may not be records, but documents), and the latest version is being transferred to a new RMA [possibly from a document management application (DMA)]. When a user opens up an outdated version of that document, the system should indicate that the latest version is located in the RMA.	**4**			Cannot ensure that records are disposed of properly.	

Criterion	Risk Baseline	Compliance Value	Risk Score	Adverse Effect	Comment
1.6.6 Unique identifiers are transferred from source systems to the RMA (i.e., the system sends the unique identifier for a record from the original system to the RMA when a record is transferred to the RMA).	**4**			Cannot ensure that records are disposed of properly.	
Class Summary	***26***				

Appendix J—ERK System Certification Report Template

Electronic Recordkeeping (ERK)

System Certification Report

<System Name>

<System Acronym>

[date]

Version

Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20530

Prepared by Electronic Records Section Staff
[Name], Test Team Leader
Reviewed by [Reviewer's Name]

Table of Contents

List of Tables

1. Purpose of Document

[Describe the purpose of the document and provide a brief description of the system compliance evaluation process. Sample text follows.]

The purpose of the ERK System Certification Report is to compile and convey the results of the electronic recordkeeping certification (ERKC) Validation process for the <system name (acronym)>. The Validation process consists of an evaluation of the system against FBI ERK Assessment Criteria. The evaluation determines how well the characteristics of the system satisfy the ERK criteria.

The criteria are listed in the ERK Compliance Evaluation Worksheet. Each criterion has a pre-assigned Risk Baseline Value to denote how critical it is with regard to electronic recordkeeping. If the system completely satisfies a criterion, the Compliance Value is 1 (i.e., 100 percent of the Baseline Value). If the criterion is not completely satisfied by the characteristics of the system, the Evaluator judges how close the system comes to satisfying the criterion and assigns a decimal score ranging from 0 to 1, with 1 signifying 100 percent compliance. If the criterion is not relevant to the system, the Evaluator assigns a Risk Baseline value of 1.

2. Description of <System>

[Provide a brief description of the system, including the system name, the FBI Section and Division to which it belongs, its purpose, and a description of the records that it contains.]

3. System Risk Assessment

[Provide a general description or summary of the system's compliance and non-compliance with ERK criteria.]

3.1 Summary of Compliance Evaluation Scores

The following table summarizes the ERK Compliance Evaluation scores for <system> by criteria class.

Table 3-1. Compliance Evaluation Scores Summary

Criteria Class	Total Baseline Value for the Class	Score
Declare Records	14	
Capture Records	6	
Records Organization	30	
Records Security	22	
Records Access	11	
Records Retrieval	10	
Records Preservation	13	
Audit/Oversight	11	

Criteria Class	Total Baseline Value for the Class	Score
Dispose of Records	18	
Process Records Containing Restricted or National Security Classified Data	16	
Interface with Records Management Application	26	
Total Risk Score	177	

[Highlight areas of exceptionally strong or poor compliance]

The following sections describe system non-compliance with ERK criteria. These descriptions are organized by ERK criteria class. Appendix A of this System Certification Report provides the completed ERK Compliance Evaluation Worksheet, which provides additional details of the evaluation. For each instance of non-compliance, the following items are presented:

- Detailed description of non-compliance
- Recommendations to achieve compliance
- Potential consequences of non-compliance
- Mitigating circumstances, if any

3.2 Declare Records

3.3 Capture Records

3.4 Maintain or Use Records

3.4.1 Records Organization

3.4.2 Records Security

3.4.3 Records Access

3.4.4 Records Retrieval

3.4.5 Records Preservation

3.4.6 Audit/Oversight

3.5 Dispose of Records

3.6 Process Records Containing Restricted or National Security Classified Data

3.7 Interface with Records Management Application (RMA)

Appendix A: ERK Compliance Evaluation Worksheet

<insert Worksheet>

Appendix K—ERK Certification Letter Template

U.S. Department of Justice
Federal Bureau of Investigation
Washington, DC 20535-0001

<Date>

<Name>
AD, <System Owner division>
Federal Bureau of Investigation
Room
Washington, DC 20535

Dear (name):

The purpose of this communication is to certify the <named information system (acronym)> to be in compliance with the electronic recordkeeping. The Records Management Division has completed the review of the ERK System Certification Report dated <date> and received <date>.

The FBI Records Officer, in conjunction with the Records Management Division, has determined that the system [is approved to operate.] [has an interim approval to operate. The interim approval to operate is contingent on the action items being achieved within the next 180 days.]

The Records Management Division evaluated the <system acronym> for compliance with regulations from the National Archives and Records Administration (NARA), in concert with FBI policy. Certification is granted for the period of three years or until major changes affecting the records profile of the system are made. The ERK certification is in effect from <date> to <date>.

CERTIFICATION STATEMENT FOR
<NAMED INFORMATION SYSTEM (ACRONYM)>

Sincerely,

Robert Garrity
FBI Records Officer

Case ID#:

Appendix L—Sample ERKC Electronic Communication Template

Electronic Recordkeeping Certification Electronic Communication (EC)

FEDERAL BUREAU OF INVESTIGATION

Precedence: Routine **Date:**

To: System Owner Division **Attn:** AD, System Owner Division
POC(s) System Owner Division

Records Management Division **Attn:** AD, Records Management Division
AD, Information Resources Division

From: Records Management Division
Contact: Michael L. Miller, <ext #>

Approved By: Robert Garrity,

Drafted By: <name>

Case ID #:

Title: CREDITATION – RECOMMENDATION FOR ERK CERTIFICATION OF THE NAMED INFORMATION SYSTEM (ACRONYM)

Synopsis: To notify the System Owner of the certification of the of the <names information system (acronym)> [and address outstanding items].

Reference: <number> Serial No. (Certification EC)

Details: The Records Management Division has completed the review of the <system's acronym> ERK Compliance Evaluation Report dated <date> and received <date>. Resulting from this review, the Records Management Division has recommended that the <system acronym> be ERK certified from <date> to <date>.

[The <system acronym> certification is contingent on [list vulnerabilities and required actions] to be completed within 180 days. Maintaining a current certification is also subject to the continued adherence to the provisions of ERK certification criteria.]

LEADS:

Set Lead 1: (Action)
System Owner Division at Washington, DC

Develop and implement [required corrective actions] within 180 days.

Appendix M—FBI RMA Metadata List

Element	*Definition/Descriptions*
Individual Documents	
Unique RMA Identifier	An unambiguous system-generated data element that identifies a particular record.
Contributor Record ID	Unique ID provided by the Contributing System which identifies a particular record within that system.
File Number	Identifies the classification, sub-classification (alpha), Office of Origin, and Case number.
Serial	Number assigned to the document within the Case ID.
Document Type	Code indicating the type of document. "TYPE"
Document Date	Generally the date appearing on the face of the document. In the case of e-mail, it is date sent.
To / Addressee	The recipient(s) of the document.
From / Author – Individual	The originator of the document. The individual who creates, sends, signs the document.
From / Author – Organization	The organization to which the originator of the document belongs.
Title / Subject / Topic of Document	Generally the "name" of the document (e.g., the title of an EC or memorandum, the subject line of an e-mail, the title of a report, briefing, spreadsheet, etc.)
Description / Abstract / Notes	A brief narrative description about the record, which usually contains keywords.
National Security Classification	Identifies the classification level for the security classification. The document classification reflects the highest classification in the document.
Other Restrictions	Identifies a record to which a legislative or regulatory restriction has been applied (i.e., Rule 6(e), FOIA, litigation matters).
Record Status	Indicates the distinction between the official record, a copy, duplicates, etc. The default would be Records. Generally inherited from the file classification or file number.
Document Disposition	Those actions taken regarding Federal records after they are no longer required to conduct current Agency business. Generally inherited from the file classification or file number.
File Classification Disposition	The disposition assigned to the file classification number. Can be permanent, disposable, sample/select – undetermined, sample/select – permanent, sample/select – disposable, or unscheduled.
Selection Criteria	If the disposition is sample/select – permanent, this identifies the criterion/criteria used to make that determination.
Records Schedule Identification	Identification of the approved disposition authority. Generally linked from the file classification.
Entry Date	The date the record was entered into the system.
Batch Documents (Managed at the file level or higher)	
Individually Entered Data Elements	
File Number	Identifies the classification, sub-classification (alpha), Office of Origin, and Case number
Volume Number / Sub-part of the Case File	Identifies the location of the record within the sub-sets of a physical case file.

Batch Generated Data Elements	
Record Status	Indicates the distinction between the official record, a copy, duplicates, etc. The default would be Records.
Document Disposition	Those actions taken regarding Federal records after they are no longer required to conduct current Agency business. Generally inherited from the file classification or file number.
File Classification Disposition	The disposition assigned to the file classification number. Can be permanent, disposable, sample/select – undetermined, sample/select – permanent, sample/select – disposable, or unscheduled.
Selection Criteria	If the disposition is sample/select – permanent, this identifies the criterion/criteria used to make that determination.
Retention	The length of time that a record must be kept before it is destroyed, which is determined by scheduling.
National Security Classification	Identifies the classification level for the security classification. The document classification reflects the highest classification in the document.
Other Restriction	Identifies a document to which a legislative or regulatory restriction has been applied, (i.e., Rule 6(e), FOIA, litigation matters).
Scanning Project ID	Identifies the title of the Scanning Project.
System Generated Data Elements	
Unique RMA Identifier	An unambiguous system-generated data element that identifies a particular record.
Entry Date	The date the record was entered into the system.