



# U.S. FISH AND WILDLIFE SERVICE TRANSMITTAL SHEET

PART 270 FW 4	SUBJECT ITM Program Management Management Control Reviews of Automated Information Systems	RELEASE NO. FWM 455
FOR FURTHER INFORMATION CONTACT Division of Information Resources Technology Mgt.		DATE 09/29/04

## EXPLANATION OF MATERIAL TRANSMITTED:

This is a minor revision of 270 FW 4, which establishes policies and procedures for performing management control reviews of automated information systems in the Service.

  
Acting  
DIRECTOR

---

## FILING INSTRUCTIONS:

Remove:

270 FW 4, 09/30/02, FWM 406

Insert:

270 FW 4, 09/29/04, FWM 455

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 270 ITM Program Management**

**Chapter 4 Management Control Reviews of Automated Information Systems**

**270 FW 4**

**4.1 What is the purpose of this chapter?** This chapter establishes policies and procedures for performing Management Control Reviews (MCR) of automated information systems in the Service. These reviews are part of an overall risk management strategy and will determine if systems are operating within an acceptable level of risk. The review process addresses management controls, practices, and policies as well as associated technical issues. Regular reviews will result in the early identification of potential problems and permit more cost-effective remedies. A properly oriented review program will also identify beneficial policies, practices, and products that the Service could adapt and share with other users.

**4.2 Why are MCRs required for automated information systems?** Various Federal laws and policies mandate a 3-year review cycle for automated information systems.

**A.** 375 DM 5, IRM Program Review.

**B.** Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources.

**C.** OMB Circular A-127, Financial Management Systems.

**D.** 340 DM, Management Accountability and Control.

**E.** Federal Managers' Financial Integrity Act of 1982.

**F.** 290 FW 1-2, Management Control Systems.

**G.** Federal Information Security Management Act (FISMA).

**4.3 How does this chapter relate to other Service policies?** 270 FW 2 addresses the general requirements for initiating and funding a system to become part of the Service's Information Technology (IT) investment portfolio and for managing its life cycle. This chapter articulates the requirements to integrate periodic reviews into the life cycle. 270 FW 1 states policy on IT architecture with which Service systems must conform. 270 FW 7 focuses on specific IT security requirements that are a critical part of a system's life cycle.

**4.4 What are the definitions of the terms used in this chapter?**

**A. Automated Information System.** A discrete set of information and IT organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Automated information systems include both general support systems and major applications as those terms are defined in OMB Circular A-130, Appendix III. Examples are local and wide area networks, telecommunications systems, electronic mail systems, geographic information system (GIS) projects, data creation projects, databases, and radio projects.

**B. General Support System (GSS).** A term from OMB Circular A-130, Appendix III, meaning an interconnected set of information resources under the same direct management control that shares common functionality and normally includes hardware, software, information, data, applications, communications, and people. Examples are local and wide area networks, telecommunications systems, and electronic mail systems.

**C. Automated Information System Owner.** The manager who makes the decision to fund the automated information system and who is responsible for the development, acquisition, operation, and maintenance of the system.

**D. Independent Review.** A review that is conducted by a group outside of the program or Region or California/Nevada Operations Office (CNO) whose system is being reviewed.

**E. Major Application (MA).** A term from OMB Circular A-130, Appendix III, meaning an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Do not confuse this use of "major" with its use in the term "major automated information system" in 270 FW 2, OMB Circular A-11, and the body of A-130, where it designates certain levels of capital investment for a system.

**F. Management Controls.** The organization, policies, and procedures used by agencies to reasonably ensure that programs:

- (1) Achieve their intended results.
- (2) Use resources consistent with the agency mission.
- (3) Protect themselves and their resources from waste, fraud, and mismanagement.
- (4) Follow laws and regulations.
- (5) Obtain, maintain, report, and use reliable and timely information for decision making.

**G. Material Weakness.** A serious deficiency that is reported up through management levels to the Department. The Management Control and Audit Follow-Up Council determines whether or not a weakness is material and should be reported outside the Department. See 340 DM 1 and 290 FW 1.

**H. Self-Review.** A review conducted by the program or Region/CNO whose system is being reviewed.

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 270 ITM Program Management**

**Chapter 4 Management Control Reviews of Automated Information Systems**

**270 FW 4**

**4.5 What is the Service's MCR policy for automated information systems?** Annually, DOI issues a list of automated information systems that are classified as either major applications (MA) or general support systems (GSS). The automated information systems on this list will be part of the Service's MCR schedule and undergo an MCR as required by DOI and FWS policy.

**4.6 What are the major components of MCRs of automated information systems?** Reviews must adhere to the methodology in the National Institute of Standards and Technology (NIST) Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. This document contains complete guidance and a questionnaire/checklist for reviewing the controls of IT systems. Annually, the Division of Information Resources and Technology Management (IRTM) will provide an MCR package containing detailed instructions and an automated tool to produce the questionnaire.

**A. Form an MCR team.** The system owner should appoint a team and a team leader to conduct the MCR. If the MCR is a self-review, the team leader and most team members will be from the program or Region/CNO whose system is being reviewed, but it should contain at least one member from a different program or Region/CNO. If the MCR is an independent audit, the team leader and members will be from other programs and Regions/CNO, or will be contractors, but the team should contain at least one member from the program or Region/CNO whose system is being reviewed. The team conducts the onsite reviews and collects the review data.

**B. Brief the system owner.** The team leader should present a briefing to the system owner to identify review objectives and a schedule of activities, discuss the methodology, evaluate the checklists and questions, and recommend additions or modifications. The team leader will also discuss any specific areas of concern that the local managers want addressed.

**C. Review and test the system's controls.** Those responsible for conducting an MCR should follow the methodology in the NIST 800-26 questionnaire and use the automated tool provided by IRTM to produce the questionnaire. For each control on the checklist, review the controls that are in place, test the controls to determine if they are effective, and identify possible vulnerabilities. Review all documentation relevant to each item. Interview the system owners, the system manager, the system security manager, and selected users to verify answers. Document the methodology and the results obtained. The reviews should be accomplished in the most efficient manner for the program or Region/CNO, and you may use telephone interviews where appropriate. Summarize results on the checklist.

**D. Identify control weaknesses.** The team should analyze the findings from the checklist and summarize them as described by the guidance provided in the MCR package. The team should also review the findings of previous audits and reviews, as well as the system's current Plan of Actions and Milestones (POA&M) to ensure that all findings are addressed.

**E. Evaluation of results by system owner.** The team leader should brief the system owner on the results and discuss possible corrective actions.

**F. Identify corrective actions.** For each reportable control weakness, determine corrective actions and completion dates. Complete a POA&M that provides a detailed list of weaknesses and planned corrective actions.

**G. Provide the results of the MCR.** Submit the summary of findings and, if applicable, the POA&M with a cover memorandum containing the information about the review to the Chief, Division of Policy and Directives Management (Attention: Service Management Control Coordinator) with copies to IRTM. The cover memorandum must contain information as described in the instructions provided by IRTM.

**4.7 How does the Service provide detailed procedures and guidelines for conducting Information Technology MCRs?** The team members will have an orientation session prior to the start of the review process to present standards for appropriate and ethical behavior during the review and guidelines for conducting successful reviews. Topics covered during the orientation session include:

**A.** Team leaders will advise team members to look for and identify positive factors as well as noncompliance items so that the information presented to management will provide a balanced and complete representation of the environment under review.

**B.** Team leaders will prepare interview questions and checklists and advise team members to follow them as closely as possible. Gathering of collateral information is encouraged, but avoid branching off into new topic areas without prior notice to the resource manager and approval of the team leader.

**C.** During the review process, team members will refrain from conducting business not directly related to the review. Team members will not file any independent reports relative to review findings and recommendations.

**D.** Points of contact for the reviews and interviews will be obtained, times identified, and a schedule of activities developed. Every effort will be made to minimize disruption and impact on the resident workforce.

**FISH AND WILDLIFE SERVICE  
INFORMATION RESOURCES MANAGEMENT**

**Information Resources Management**

**Part 270 ITM Program Management**

**Chapter 4 Management Control Reviews of Automated Information Systems**

**270 FW 4**

**E.** Review assignments will be given and times for meetings to discuss, record, and consolidate findings will be established.

**F.** On the last day of the review, a meeting will be set for the team to brief the system owner. The findings and recommendations developed will be presented and discussed. The findings will include both positive and negative items. The team leader will provide a signed copy of findings to the system owner.

**4.8 How will corrective actions be tracked?** The Service and the Department will track corrective actions. After completion of a corrective action, the system owner will fill out and submit FWS Form 3-2147 (Certification of Completed Corrective Action) to the Service Management Control Coordinator.

**4.9 Who is responsible for implementing the provisions of this chapter?**

**A.** The Director provides the high-level visibility and support required to implement and maintain a viable and effective Information Technology Management Control Review Program.

**B. Assistant Directors and Regional Directors/CNO Manager** are responsible for:

(1) Implementing the Service's Management Control Review Program within their program or Region/CNO in accordance with this chapter.

(2) Funding reviews for MAs and GSSs as appropriate.

(3) Reviewing all findings and recommendations resulting from MCRs of automated information systems and taking action to address pertinent issues.

**C. Automated Information System Owners** are responsible for:

(1) Reporting new MAs and GSSs to IRTM. This should be part of the process described in 270 FW 2.

(2) Preparing funding requests for independent reviews of MAs and GSSs.

(3) Implementing corrective actions identified in MCRs.

**D. Chief, IRTM** is responsible for:

(1) Identifying MAs and GSSs as part of the Service's IT portfolio. See 270 FW 2.

(2) Establishing the schedule for MCRs of MAs and GSSs.

(3) Reviewing MCR reports of MAs and GSSs and

providing the Service Management Control Coordinator with comments and recommendations.

**E. The Service Management Control Coordinator** is responsible for:

(1) Coordinating with IRTM on MAs and GSSs that should be incorporated into the Service's MCR schedule.

(2) Providing IRTM copies of MCR reports for review, comments, and recommendations.

**F. MCR Team Leaders** are responsible for:

(1) Coordinating with the system owners to establish a satisfactory review schedule.

(2) Identifying personnel to be interviewed and topics of interviews.

(3) Determining local support requirements, such as personnel, equipment, office space, etc.

(4) Coordinating with system owners to select MCR teams.

(5) Developing the schedule for briefing system owners at the outset and the conclusion of MCRs.

(6) Leading the reviews and preparing reports of findings and recommendations.

(7) Preparing any required Departmental and Service reports or products.