

**SECTION 3**  
**CHAPTER 3**  
**EXECUTING INTERNAL CONTROL REVIEWS FOR INFORMATION SYSTEMS & IT PROGRAMS**

1. Policy: Internal Control Reviews (ICRs) of all information systems and Information Technology (IT) programs shall be conducted on an annual basis in accordance with and in support of Federal Managers' Financial Integrity Act of 1982, OMB Circular A-123, Federal Information Security Management Act of 2002, OMB Circular A-130, NIST Special Publications 800-26, 800-37, and 800-53.
2. Scope: All Department information systems and IT programs.
3. Definitions:
  - 3.1. The term “information system” refers to either a major application or general support system with a defined security accreditation boundary as described in the NIST “Certification and Accreditation Guide” (NIST Special Publication 800-37).
    - 3.1.1. The term “major application” means 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. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other application should be provided by security of the system in which they operate (either a major application or general support system). Source: OMB A-130 Appendix III
    - 3.1.2. The term “general support system” or “system” means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO). Source: OMB A-130 Appendix III
    - 3.1.3. The process of uniquely assigning information resources (“information resources” consist of information and related resources, such as personnel, equipment, funds, and information technology) to an information system defines the “security accreditation boundary” for that system. Source: NIST Special Publication 800-37
    - 3.1.4. Material Weakness – A reportable condition, or combination of

reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements, or other significant financial reports, will not be prevented or detected. (IC-8)

3.1.5. Non-conformance – A condition in which financial management systems do not substantially conform to financial systems requirements. Financial management systems include both financial and financially relate (or mixed) systems. The OIG often terms this as a NONCompliance issue. (IC-8)

3.1.6. Nonmaterial weaknesses – Control problems that can be corrected at the bureau/office level without the approval or attention of the next higher level or management. (IC-8)

4. Policy & Process:

\* Note: If the dates provided in the policy and process do not fall on a business day, the next business day should be used.

4.1. The OCIO ICR Coordinator shall distribute the revised assessment template and guidance document for completing the template; and shall issue a complete listing of information systems to all bureaus and offices for reconciling and baselining the information systems to be reviewed. This shall be completed during the month of January.

4.1.1. Any discrepancies between the distributed list and bureau and office lists shall be immediately resolved, and any necessary updates completed.

4.2. The Bureau and Office Chief Information Officers shall immediately begin formalizing and executing plans to review all of the information systems and IT program(s) under their responsibility. Plans shall be submitted by each Bureau and Office Chief Information Officer to the OCIO ICR Coordinator by March 1<sup>st</sup>.

4.2.1. The plans shall include all information systems and IT program(s) for the bureau or office.

4.2.2. The plans shall include a reasonable schedule with defined dates and the appropriate designated resources for each of the major functions of the ICR.

4.2.3. The plans shall demonstrate a schedule that meets the date requirements for delivery of the reports to the department.

4.3. ICRs for all Information Systems and IT programs shall be completed and submitted to the OCIO ICR Coordinator by June 1<sup>st</sup>.

4.3.1. The ICR of each Information System shall include:

4.3.2. a completed NIST Special Publication 800-26, or a revised 800-26 self assessment questionnaire;

- 4.3.2.1. The guidance and instructions in NIST Special Publication shall be followed to ascertain and conclude the maturity level of the program and information systems for each control area.
- 4.3.3. A statement letter of “No Weaknesses” or “Weaknesses Found.” Statement letters shall be addressed to the Departmental CIO and OCIO ICR Coordinator. A separate statement letter shall be completed for each individual Information System and IT program.
  - 4.3.3.1. All Material Weaknesses, Non-conformance, and Nonmaterial Weaknesses found shall be recorded in the statement letter and recorded in the respective Information System or IT program Plan of Actions and Milestone (POA&M) report.
    - 4.3.3.1.1. A POA&M is used to identify, prioritize, and manage corrective efforts associated with the mitigation of security weaknesses identified in a system or program. It is also used to report the status of security weakness remediation efforts to OMB and Congress.
    - 4.3.3.1.2. A POA&M entry shall be made for each weakness and shall include the related corrective actions, the scheduled completion date for correcting each weakness, and the status for correcting each weakness.
- 4.4. The OCIO ICR Coordinator shall validate that ICRs have been submitted for each system identified in the list completed in §4.1. This shall be completed by June 5<sup>th</sup>. Any missing ICRs shall be announced to the respective Bureau or Office IT Security Manager and Bureau or Office Chief Information Officer.
- 4.5. The OCIO ICR Coordinator shall assess all ICRs for quality and completeness with the respective System Security Officers, System Managers, Systems Owners, and Bureau and Office IT Security Managers. This quality review shall be completed by July 1<sup>st</sup>. Within 7 business days, a letter from the OCIO ICR Coordinator, addressed to the Departmental Chief Information Officer, shall attest that all ICRs have been completed for information systems and IT programs, and all ICRs shall be included in the transmittal.

#### Bureau and Office Assurance Statements

- 4.6. All bureau and office ICRs over financial reporting shall be completed on or before June 1<sup>st</sup>. This includes required reviews for financial information systems. Bureaus’ and offices’ assurance statements over financial reporting as of June 30<sup>th</sup> must be submitted to PFM on or before June 1. The assurance statement must address compliance with FFMIA for financial Information Systems. (PFM Guidance)

- 4.6.1. POLICY: On or before June 1<sup>st</sup>, bureau and office CIOs shall sign the bureau/office assurance statement or submit a separate assurance statement. The assurance statement shall include the results of the ICR(s) and any weaknesses found for financial information systems.
- 4.7. All reviews of non-financial programs or operations planned shall be completed on or before August 31<sup>st</sup>. Bureaus' and offices' annual assurance statement over all programs and operations, including Information Systems, as of September 30<sup>th</sup>, must be submitted to PFM on or before September 15<sup>th</sup>. This statement should include an update to the June 30<sup>th</sup> assurance statement over financial reporting which verifies that key financial reporting controls either have no reportable changes between June 30<sup>th</sup>, and September 30<sup>th</sup>, or reportable material weaknesses have been corrected. (PFM Guidance)
- 4.7.1. POLICY: On or before September 15<sup>th</sup>, bureau and office CIOs shall sign the bureau/office assurance statement or submit a separate assurance statement. The assurance statement shall include the results of the ICR(s) and any weaknesses found for all Information Systems and IT programs reviewed, and any updates from the June 30<sup>th</sup> assurance statement.