



# Management Directive

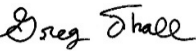
## Commonwealth of Pennsylvania

### Governor's Office

---

## Management Directive 325.03 Amended – Performance of Audit Responsibilities

Date: August 30, 2022

By Direction of:   
Greg Thall, Secretary of the Budget

Contact Agency: Office of the Budget (OB)  
Office of Comptroller Operations  
Bureau of Audits (BOA)  
Telephone 717.787.6496

**This directive establishes policy, responsibilities, and procedures for the performance of Audits, Attestation Engagements, and Non-Audit Services for Commonwealth agencies. This amendment updates definitions, policy, responsibilities, and procedures and incorporates content from the now rescinded *Management Directive 325.6 Amended, Auditing Computer Based Systems.***

### 1. PURPOSE.

To establish policy, responsibilities, and procedures for the performance of Audit, Attestation Engagements, and Non-Audit Services for Commonwealth agencies.

### 2. SCOPE.

This directive applies to all departments, offices, boards, commissions, and councils under the Governor's jurisdiction (hereinafter referred to as "agencies"). Entities not under the Governor's jurisdiction are encouraged to adopt similar policies.

### 3. OBJECTIVES.

- a. To ensure OB Audit Organizations, Agency Audit Organizations, and External Qualified Auditors understand the policy, responsibilities, and procedures established for performing Audits, Attestation Engagements, and Non-Audit Services.
- b. To ensure that Audits, Attestation Engagements, and Non-Audit Services:
  - (1) Are performed by Agency Audit Organizations or External Qualified Auditors, if delegated by OB, BOA.

- (2) Are planned and administered in an efficient, economical, and effective manner.
- (3) Are not duplicated or have gaps in coverage.
- (4) Provide reasonable assurance that the business processes and applications carry out the policies management has prescribed for them.
- (5) Document the internal controls and Audit Trails needed for management, auditor, and operational review.
- (6) Include evaluation and testing of internal controls necessary to ensure propriety of data and protection against loss, serious error, or disclosure of confidential information.
- (7) Conform to legal requirements.
- (8) Are documented in a manner that will provide the understanding of the system required for effective development, maintenance, and auditing.

#### 4. DEFINITIONS.

- a. **Agency Audit Organization.** Agency staff, organized independently of other agency organizations, programs, activities, and functions to be examined; responsible for ensuring Audits, Attestation Engagements, and Non-Audit Services are conducted objectively.
- b. **Attestation Engagement.** Attestation Engagements cover a broad range of financial and nonfinancial objectives and may provide different levels of assurance about the subject matter or assertion depending on the user's needs. The three types of Attestation Engagements are:
  - (1) **Examination.** Obtaining reasonable assurance by obtaining sufficient, appropriate evidence about the measurement or evaluation of subject matter against criteria in order to be able to draw reasonable conclusions on which to base the auditor's opinion about whether the subject matter is in accordance with (or based on) the criteria or the assertion is fairly stated, in all material respects.
  - (2) **Review.** Obtaining limited assurance by obtaining sufficient, appropriate Review evidence about the measurement or evaluation of subject matter against criteria in order to express a conclusion about whether any material modification should be made to the subject matter in order for it to be in accordance with (or based on) the criteria or to the assertion in order for it to be fairly stated. Review-level work does not include reporting on internal control or compliance with provisions of laws, regulations, contracts, and grant agreements.
  - (3) **Agreed-Upon Procedures.** Performing specific procedures on a subject matter or an assertion and reports the findings without providing an opinion or a conclusion on it. The engaging party is required to agree to the procedures and acknowledge that the procedures performed are appropriate for the intended purpose of the engagement prior to issuance of the practitioner's Agreed-Upon Procedures report.

- c. **Audit.** Financial or Performance Audits conducted in accordance with [Government Auditing Standards](#).
- (1) **Financial Audit.** Provide independent assessment of and reasonable assurance about whether an entity's reported financial condition, results, and use of resources are presented fairly in accordance with recognized criteria. Financial Audits under [Government Auditing Standards](#) include:
- (a) **Financial Statement Audit.** A Financial Audit conducted to provide reasonable assurance about whether the financial statements of the audited entity are presented fairly in all material respects in conformity with Generally Accepted Accounting Principles (GAAP), or other bases of accounting. Audits conducted also include reports on internal control over financial reporting and on compliance with provisions of laws, regulations, contracts, and grant agreements that have a material effect on the financial statements.
- (b) **Other Types of Financial Audits.** Other Types of Financial Audits provide different levels of assurance and entail various scopes of work, including, but not limited to:
- 1** Obtaining sufficient, appropriate evidence to form an opinion on a single financial statement or specified elements, accounts, or line items of a financial statement.
  - 2** Issuing letters (commonly referred to as comfort letters) for underwriters and certain other requesting parties.
  - 3** Auditing applicable compliance and internal control requirements relating to one or more government programs.
  - 4** Conducting an Audit of internal control over financial reporting that is integrated with an Audit of financial statements (integrated Audit).
- (2) **Performance Audit.** Provide objective analysis, findings, and conclusions to assist management and those charged with governance and oversight, with, among other things, improving program performance and operations, reducing costs, facilitating decision making by parties responsible for overseeing or initiating corrective action, and contributing to public accountability.
- d. **Audit Trail.** A documented series of steps or progressions that facilitate the tracing of a transaction from its initiation through all intermediate processing routines to its point of final disposition.
- e. **Commonwealth Audit Committee.** The enterprise level committee responsible to strengthen the governance and independent oversight of financial reporting and Audit processes for agencies. This committee is comprised of members designated by the Governor and, at a minimum, includes the Secretary of Budget; Secretary of Administration; the Secretary of Planning and Policy, Office of the Governor; Special Advisor to the Budget Secretary, or designee; and the State Inspector General.

- f. Computer-Based System.** An organized and interrelated group of Information Technology (IT) components including the processes, people, infrastructure, organization, and architecture, linked together according to a plan to achieve a specific objective. For the purposes of this directive, Computer-Based System collectively refers to but is not limited to the following:
- (1) **Information** as defined in *Management Directive 210.12 Amended, Electronic Commerce Initiatives and Security*.
  - (2) **Information Systems** as defined in *Information Technology Policy (ITP) BUS008, Enterprise Employment Application Policy*.
  - (3) **Information Technology** as defined in *ITP BUS 000, Information Technology Policy Governance*.
  - (4) **Business Productivity Tools** as defined in *Management Directive 205.43 Amended, Quality Assurance for Business Productivity Tools*.
  - (5) **Information Security** related to [United States Code 44, Chapter 35, Subchapter II, 44 U.S.C. §§ 3551 – 3559](#), and the [National Institute of Standards and Technology \(NIST\) Special Publication 800-39](#).
  - (6) **Artificial Intelligence (AI)** as defined in *ITP BUS012, Artificial Intelligence General Policy*.
  - (7) **Activity.** A set of actions designed to achieve a particular result. Activities are usually defined as part of processes or plans and are documented in procedures ([Information Technology Infrastructure Library \(ITIL\) Framework](#)).
  - (8) **Capability.** The ability of an organization, person, process, application, IT service, or other configuration item to carry out an activity within the [ITIL Framework](#).
- g. External Qualified Auditors.** Certified Public Accountants (CPAs) or public accountants registered under *the CPA Law, Act of May 26, 1947, P.L. 318, as amended, 63 P.S. §§ 9.1-9.16b*, and other professional consulting firms performing Audits and Attestation Engagements in accordance with [Government Auditing Standards](#).
- h. Government Auditing Standards.** A publication issued by the U.S. Government Accountability Office, Comptroller General of the United States, within which Generally Accepted Government Auditing Standards (GAGAS) are promulgated, providing guidance for auditors and Audit organizations outlining the requirements for Audit reports, professional qualifications for auditors, and Audit organization quality controls. Auditors of federal, state, and local government programs use these standards to perform their Audits and produce their reports. Commonly referred to as the "Yellow Book."
- i. Non-Audit Services.** Other activities performed by auditors that do not meet the definition of an Audit or Attestation Engagement. Examples include, but are not limited to, evaluation of internal controls; providing assistance or technical expertise; providing information or data without auditor verification of the data; and providing investigative or oversight assistance.
- j. OB Audit Organizations.** BOA and the Governor's Budget Office, Bureau of Revenue, Capital and Debt, Redevelopment Assistance Capital Program.

## 5. POLICY.

- a. Pursuant to *Section 611 of The Administrative Code of 1929, Act of April 9, 1929, P.L. 177, No. 175, as amended, 71 P.S. § 231*, the Secretary of the Budget has the authority to initiate and conduct evaluations of the effectiveness and efficiency of programs supported by an agency and to direct, coordinate, assist, or advise any agency in the conduct of evaluations of its programs or of programs which it supports.
- b. Audits and Attestation Engagements of agencies, programs, activities, functions, and Computer-Based Systems are to be performed by OB Audit Organizations, Agency Audit Organizations and External Qualified Auditors and must be performed in accordance with GAGAS as published in [Government Auditing Standards](#).
- c. Agencies shall perform Audits and Attestation Engagements of programs, activities, functions, and Computer-Based Systems:
  - (1) As mandated by funding, programmatic, legislative, and similar requirements.
  - (2) As deemed necessary in addressing issues including, but not limited to:
    - (a) Noncompliance, failure or suspected failure of internal controls.
    - (b) Fraud or suspected fraud.
    - (c) In the event of compromised or suspected compromise of Computer-Based Systems (through a breach in a connected system or resulting from third-party access), agencies must follow the processes for reporting an incident or suspected incident as outlined in *ITP-SEC024 IT Security Incident Reporting Policy* and the Incident Response Process Document. Agencies may not proceed with an audit and attestation engagement until after the conclusion of the security incident investigation.
  - (3) In accordance with this directive.
- d. BOA shall perform Audits, Attestation Engagements and Non-Audit Services of agencies, programs, activities, functions, and Computer-Based Systems as directed by the Commonwealth Audit Committee; required, deemed necessary, or due to an agency request and in collaboration with the Office of the Budget, the Commonwealth Audit Committee; and in accordance with this directive.
- e. BOA will collaborate with the Office of Administration, Information Technology (OIT) for the provision of information on Computer-Based Systems from applicable OIT reporting systems necessary to fulfill Audit responsibilities in adherence to this directive. If complete information is not available in applicable OIT reporting systems, agencies shall provide that information at BOA's request.
- f. Agencies may not contract for Audits and Attestation Engagements unless such action has been approved and formally delegated by BOA.
- g. In addition to any other requirements identified in BOA's engagement letter, agencies shall adhere to the timelines regarding document requests and meetings identified in BOA's engagement letter, unless an alternative timeline is agreed upon by the agency and BOA.

- h. [Government Auditing Standards](#) do not apply to Non-Audit Services. Therefore, when performing Non-Audit Services, auditors should not report that the Non-Audit Services were conducted in accordance with [Government Auditing Standards](#). Auditors must evaluate whether providing Non-Audit Services creates a threat to independence of mind and in appearance with respect to any GAGAS Audit or Attestation Engagement performed.
- i. Audits and Non-Audit Services apply to Computer-Based Systems in design, development, and operation phases in accordance with applicable ITPs including, but not limited to, *ITP BUS001, IT Planning and Projects, ITP SEC040, IT Service Organization Management and Cloud Requirements* and *ITP BUS012, Artificial Intelligence General Policy* as well as *Management Directive 205.43 Amended, Quality Assurance for Business Productivity Tools*.
- j. Agency Audit Organizations shall be organized independent of the programs, activities, and functions to be examined, as a means of ensuring the objectivity of all Audits and Attestation Engagements conducted.

## 6. RESPONSIBILITIES.

### a. Agency Heads.

- (1) Ensure that Agency Audit Organizations and External Qualified Auditors perform Audits, Attestation Engagements and Non-Audit Service in accordance with this directive.
- (2) Ensure BOA is notified of all Audits being performed of agency programs and operations.
- (3) Ensure BOA is notified of all activities and development of new and revisions or enhancements of existing Computer-Based Systems in accordance with ITPs.
- (4) Provide timely notice to BOA prior to the start of the Audit, Attestation Engagements, and Non-Audit Services, and periodic updates on progress and any significant issues to be included in the report.

### b. OB Audit Organizations.

- (1) Perform, at the direction of the Commonwealth's Audit Committee and through coordination with Agency Audit Organization, where applicable, risk-based, requested, and mandated Audits, Attestation Engagements, and Non-Audit Services of agency programs, activities, and operations.
- (2) Ensure that Audits, Attestation Engagements, and Non-Audit Services are performed in accordance with established policy, procedures, regulations, and applicable auditing standards.
- (3) Report agency Audits to the Commonwealth Audit Committee and the External Qualified Auditors as requested.

- c. **Agency Audit Organizations and External Qualified Auditors.** Perform Audits, Attestations Engagements, and Non-Audit Services in accordance with this directive.

## 7. PROCEDURES.

### a. Agency Heads.

- (1) Delegate agency Audit responsibility to Agency Audit Organizations and External Qualified Auditors in accordance with this directive.

- (2) When requested by BOA in accordance with 7.d(3) of this directive, provide a listing of all Audits of agency programs, operations, and Computer-Based Systems that have been completed or are in process.
- b. **OB Audit Organizations.** Monitor to ensure that Audits, Attestation Engagements, and Non-Audit Services are performed in accordance with established policy, procedures, regulations, and applicable auditing standards.
- c. **Agency Audit Organizations and External Qualified Auditors.** Perform Audits, Attestation Engagements, and Non-Audit Services in accordance with policy contained in this directive, as assigned.
- d. **BOA.**
  - (1) If requested by an agency and the capacity is available, include the Audit, Attestation Engagement or Non-Audit Service in the BOA Annual Audit Plan.
  - (2) If requested by an agency and the capacity is not available, delegate the Audit, Attestation Engagement or Non-Audit Service to External Qualified Auditors in accordance with the relevant Department of General Services procurement procedures.
  - (3) Obtain a listing of audits completed and in process from agencies for reporting to the Commonwealth Audit Committee and External Qualified Auditors as requested.

**This directive replaces, in its entirety, *Management Directive 325.3 Amended*, dated January 10, 2011, and *Management Directive 325.6 Amended*, dated January 10, 2011, which is now rescinded.**