Management Directive
Commonwealth of Pennsylvania
Governor's Office

Management Directive 325.13 Amended – Service Organization Controls

Date: February 15, 2024

By Direction of:

Uri Z. Monson, Secretary of the Budget

Contact Agency: Office of the Budget
Office of Comptroller Operations
Bureau of Quality Assurance
Telephone: 717.787.6496

This directive establishes policy, responsibilities, and procedures for the oversight and evaluation of a Service Organization's Internal Controls. This amendment updates the contact agency, references appropriate information technology policies (ITPs), and updates definitions and formatting.

1. PURPOSE.

To establish policy, responsibilities, and procedures for the oversight and evaluation of a Service Organization's Internal Controls.

2. SCOPE.

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

3. OBJECTIVE.

To ensure the integrity of governmental functions, processes, or data provided or maintained by Service Organizations.

4. DEFINITIONS.

a. Internal Control. A process effected by an agency that provides reasonable assurance that objectives are being achieved.

b. **Service Organization.** A party external to Commonwealth government that provides operational processes (e.g., claims processing, hosting data centers, provision of cloud-based services) for an agency.

5. POLICY.

a. Agencies are responsible for the processes assigned to Service Organizations that are likely to be relevant to the agency's Internal Control. This responsibility includes oversight of each Service Organization's Internal Controls.

b. Agencies must consider the following when determining the extent of oversight for the processes assigned to Service Organizations:

(1) The nature of services outsourced.

(2) The standards of conduct of the Service Organization's personnel.

(3) The quality and frequency of the Service Organization's enforcement of adherence to standards of conduct by its personnel.

(4) The magnitude and level of complexity of the Service Organization's operations and organizational structure.

(5) The extent to which the Service Organization's Internal Controls are sufficient so that the agency and the Service Organization achieve their objectives and address risks related to the assigned operational process.

c. Agencies' oversight of Service Organizations can include defined monitoring activities, independent audits or other assessments, or a combination of both.

d. Agencies must understand the controls that each Service Organization maintains, as well as how each Service Organization's Internal Control system interacts with the agency's Internal Control system.

e. Agencies must ensure that proper contingency plans are in place in the event that a Service Organization's ability to provide services critical to the agency's core functions, processes, or data is compromised.

f. Agencies shall adhere to information technology policies (ITPs) that are issued by the Office of Administration addressing Service Organizations, as appropriate, including but not limited to, *ITP-SEC040, Computing Services Provided by Service Organizations*, its attachments, and additional ITPs that reference this specific ITP.

6. RESPONSIBILITIES.

a. Agencies shall:

(1) Identify Service Organizations within their purview.

(2) Evaluate appropriate levels of oversight, as well as determine which monitoring requirements, independent audits, or assessments are needed to confirm the operating effectiveness of a Service Organization's Internal Control system.

(3) Integrate monitoring, independent audit, and assessment activities into the contract process as appropriate, including:

(a) Defining required monitoring reports and on-site activities during the procurement process.

(b) Alerting potential Service Organizations to the need for independent audits or assessments during the procurement process.

(c) Assessing a potential Service Organization's ability to provide independent audits or assessments.

(d) Including independent audits or assessments in contract requirements.

(4) Communicate monitoring, audit, or assessment findings to Service Organizations.

(5) Develop, implement, and monitor corrective action plans based on monitoring, audit, or assessment findings, as needed.

(6) Develop up-to-date contingency plans for services provided by Service Organizations that are critical to the agency's core functions, processes, or data.

b. Office of the Budget, Office of Comptroller Operations shall:

(1) Assist agencies with determining the most appropriate monitoring, audit, or assessment type needed.

(2) Distribute resulting monitoring, independent audits, examinations, or assessments to the Commonwealth's external auditors as necessary.

7. PROCEDURES.

Agencies.

a. Identify all Service Organizations.

(1) Review all current and future vendor contracts and relationships and determine if each vendor meets the definition of a Service Organization.

(2) Maintain a record of each Service Organization and the services they provide.

b. Determine level of oversight.

(1) Review services provided by Service Organizations.

(a) Note critical or sensitive services (e.g., financial transaction processing, data processing, or hosting).

(b) Note any subservice organizations, as well as the services they provide.

(c) Note any Federal oversight requirements.

(2) Compare services against list of oversight options (see "Guidance on Oversight Options for Service Organizations").

(3) Select the most appropriate oversight option and maintain evidentiary documentation to support their selected oversight option.

c. Execute oversight plan.

(1) Identify vendor reporting requirements based on selected oversight option.

(2) Ensure timely Service Organization reporting.

(3) Ensure compliance with contract requirements.

(4) Consider including selected oversight option and reporting requirements in the Service Organization contract.

This directive replaces, in its entirety, *Management Directive 325.13,* dated November 22, 2017.