



Management Directive

Commonwealth of Pennsylvania

Governor's Office

Management Directive 325.12, Amended – Standards for Enterprise Risk Management in Commonwealth Agencies

Date: October 1, 2021

By Direction of: *Greg Thall*
Greg Thall, 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 implementing an Enterprise Risk Management (ERM) framework within Commonwealth agencies. This amendment broadens the focus of the previous directive as the Commonwealth implements an ERM framework. Definitions, policy, and responsibilities have all been updated to reflect the new ERM framework. [The ERM Guide](#), which provides additional information and specific procedural guidance, is incorporated by reference.

1. PURPOSE.

To establish policy, responsibilities, and procedures for implementing an ERM framework within agencies.

2. SCOPE.

This directive applies to all departments, offices, boards, commissions, and councils (hereinafter referred to as "agencies") under the Governor's jurisdiction.

3. OBJECTIVES.

To adopt and implement an ERM framework that will ensure agencies have a coordinated, consistent, and practical methodology to identify, analyze, and respond to Risks through the effective application of Internal Controls.

4. DEFINITIONS.

- a. **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.
- b. **Commonwealth Chief Risk Officer (CRO).** The enterprise level executive responsible for leading the enterprise ERM approach and activities.
- c. **Control Deficiency.** When the design, implementation, or operation of an Internal Control does not allow agency personnel, in the normal course of performing their assigned functions, to achieve objectives and address related Risks.
- d. **Enterprise Risk Management (ERM).** The coordinated application of Risk Management and Internal Control activities within the Commonwealth, the goal of which is to ensure agencies have a consistent method to identify, analyze, and respond to Risks by the application of effective Internal Controls.
- e. **Green Book.** The commonly used name for the *Standards for Internal Control in the Federal Government* issued by the United States Government Accountability Office. The Green Book provides Management with criteria to design, implement, and operate effective Internal Controls.
- f. **Internal Control.** A process effected by an agency that provides reasonable assurance that objectives are being achieved.
- g. **Management.** Agency personnel who are directly responsible for the activities of a program or objective, including the identification of, analysis of, and response to Risks as well as the design, implementation, and operating effectiveness of Internal Controls.
- h. **Oversight Body.** The designated members of an agency's senior Management team responsible for overseeing Management's implementation of the ERM framework.
- i. **Risk.** Any internal or external event that could affect an entity's ability to achieve its business objectives, vision, or mission.
- j. **Risk and Compliance Officer (RCO).** The agency executive responsible for leading the agency's ERM approach and activities.
- k. **Risk Assessment.** A periodic process to identify, analyze, and document responses to Risk.
- l. **Risk Management.** The ongoing process of identifying and analyzing an organization's Risks, developing responses to those Risks, and improving deployment of resources.
- m. **Service Organization.** A party external to Commonwealth government that provides operational processes for an agency.

5. POLICY.

- a. ERM activities shall be overseen by the Commonwealth Audit Committee but directed and managed by the CRO and individual agency leadership.
- b. An Oversight Body must be appointed by the agency head to oversee the implementation and operation of the ERM framework within the agency.
- c. An agency RCO must be appointed by the agency head and provided with sufficient authority to carry out assigned responsibilities. This individual, in collaboration and consultation with the Oversight Body and agency head, shall lead the agency's ERM approach and activities.
- d. Agencies are required to conduct a comprehensive Risk Assessment of operations annually. Agency Risk Assessments must, at a minimum:
 - (1) Identify and analyze Risks across the organization.
 - (2) Determine how to respond to identified Risks.
 - (3) Identify and assess the effectiveness of Internal Controls in place to mitigate identified Risks.
 - (4) Develop and implement a monitoring plan for identified Risks.
- e. Agencies must assess the effectiveness of their Internal Controls and their adherence to the components and principles noted in the [Green Book](#). Assessments shall cover all aspects of an agency's operations, reporting and compliance with applicable laws and regulations. Results of the Internal Control assessments shall be documented within a report titled the [Enterprise Risk Management Report \(ERM Report\)](#) in accordance with this directive and [The ERM Guide](#).
- f. Agencies must maintain adequate written documentation for activities conducted in connection with Risk Assessments, review of Internal Controls and follow-up actions. Documentation must be available for review, upon request, by the Office of the Budget, Office of Comptroller Operations (OCO) or by the CRO.
- g. Agencies shall submit annually their [ERM Report](#) to OCO by September 30 (for the fiscal year ending June 30).

6. RESPONSIBILITIES

- a. **Agency Heads** shall:
 - (1) Establish an Oversight Body and appoint an RCO with sufficient authority to carry out assigned responsibilities.
 - (2) Establish agency policies and procedures to ensure the effective design, implementation, and operation of Internal Controls in accordance with this directive.
 - (3) Ensure that Risk information and analysis are incorporated into strategic and operational decision-making and utilized throughout the agency.

- (4) Ensure the completion and submission of the agency's annual [ERM Report](#) in accordance with this directive and [The ERM Guide](#).
- b. **RCOs** shall:
 - (1) In collaboration and consultation with the Oversight Body and agency head, lead the agency's ERM approach and activities.
 - (2) Ensure required reporting in accordance with this directive is submitted timely to OCO.
 - (3) Assist Management with the development of ERM monitoring plans.
- c. **Management** shall:
 - (1) Participate in Risk Assessment activities, including identifying and analyzing Risks.
 - (2) Develop and implement effective Internal Controls to mitigate Risk.
 - (3) Ensure employees receive information on Risk Management and Internal Controls.
 - (4) Continuously monitor and improve the effectiveness of Internal Controls associated with their operations.
 - (5) Identify and report Control deficiencies to the Oversight Body.
 - (6) Develop a corrective action plan for Control Deficiencies and monitor the progress to ensure timely and effective results.
 - (7) Follow the policy and procedures in *Management Directive 325.13, Service Organization Controls* when using Service Organizations that support agency processes.
 - (8) Implement the ERM framework where practicable.
- d. **Oversight Body** shall:
 - (1) Support Management's efforts to complete ERM activities by assigning appropriate staff and resources.
 - (2) Advise Management on how they should address both Control Deficiencies and unmitigated Risks.
 - (3) Monitor corrective actions taken by Management to confirm they have sufficiently addressed Control Deficiencies and unmitigated Risks.
- e. **OCO** shall:
 - (1) In collaboration with the CRO, provide guidance and assistance to agencies to effectively implement and maintain their ERM framework and complete necessary activities in accordance with this directive.
 - (2) Track annual submission of agencies' [ERM Reports](#).
 - (3) Review annual submissions of [ERM Reports](#) and report aggregate Internal Control issues and significant Risks to the Commonwealth Audit Committee.

- (4) Notify the Commonwealth Audit Committee of agencies that fail to provide the required ERM Reports.

f. Commonwealth Audit Committee shall:

- (1) Assess aggregate Internal Control issues and significant Risks to determine the effect on enterprise-wide objectives and whether an appropriate audit response is necessary.
- (2) Assist in prioritization of necessary resources for agencies to mitigate significant Risks and remediate aggregate Internal Control issues.

7. PROCEDURES.

Procedures and additional guidance set forth in The ERM Guide are incorporated in this directive by reference.

This directive replaces, in its entirety, *Management Directive 325.12 Amended*, dated May 15, 2018.