

Overview of Risk Assessment Forms

To comply with the Financial Integrity Act and to ensure a comprehensive system of internal control is in place and operating effectively, COSO's Enterprise Risk Management (ERM) Framework has been adopted by the State of Tennessee as the model all agencies shall follow. Conveniently, the eight ERM components correlate with the five components illustrated in the September [2014 revision of the Standards for Internal Control in the Federal Government](#), also known as the Green Book, 'Resources' tab for crosswalk. Because the Green Book aligns with ERM and is written for a government audience, it proves to be a very useful reference tool throughout the ERM process, and is referred to often in these materials. Five forms have been developed to facilitate the process of evaluating and documenting the extent to which your organization has implemented the eight components of COSO's Enterprise Risk Management – Integrated Framework. Agencies are not required to use these specific forms, but must comply with the requirements of the Financial Integrity Act (*Tennessee Code Annotated* Title 9, Chapter 18).

The five forms that may be used are as follows:

Form 1 – ERM Component: Internal Environment

Form 2 – ERM Component: Objective Setting

Form 3 – ERM Components: Event/Risk Identification, Risk Assessment, Risk Response, Control Activities

Form 4 – ERM Component: Information and Communication

Form 5 – ERM Component: Monitoring

The five components of internal control illustrated in the revised Green Book are further broken down into 17 principles, and finally into multiple attributes that support the design and implementation of each principle of internal control. Each of the five forms is labeled in the heading with the ERM components covered by the form, and most forms include the specific Green Book principles and attributes supporting each component, but users are encouraged to refer to the Green Book for additional information and discussion of each principle.

Forms 1, 4, & 5 are designed to be completed in narrative format by describing how the section, office, division, or agency has incorporated each principle into the entity's existing internal control framework. These three forms should be completed by an appropriate level of management within the agency. Forms 2 and 3 are more tabular in nature, containing several individual cells that are to be completed, and should be completed in order. Specific instructions are included either within each form or within a separate document. Additionally, some forms contain examples to help the user better understand how to complete the form; these examples are not intended to be comprehensive or complete. In order to effectively complete each form, the respondent must read and understand each of the relevant Green Book principles, then contemplate various aspects of the organization, such as culture, organizational structure, policies and procedures, strength of leadership, competence of staff, quality and reliability of information systems, etc. The revised Green Book retains a specific instruction for management to consider the potential for fraud, and new instructions for management to identify, analyze, and respond to changes that could significantly impact the internal control system. These are captured in principles 8 and 9, respectively, in the Green Book and should be specifically contemplated during the risk assessment process, particularly when completing form 3.

The Green Book, beginning on page 71, outlines six minimum documentation requirements as follows:

Overview of Risk Assessment Forms

1. If management determines that a principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively. (paragraph OV2.06)

The documentation requirement above will most likely not apply to most state agencies because all principles should be relevant to all agencies. Documentation to support management's determination that a particular principle is not relevant to the organization may be included in the body of the form, when appropriate, or may be prepared in a separate document.

2. Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies on a timely basis. (paragraph 17.05)
3. Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis. (paragraph 17.06)

Documentation requirements 2 & 3 above are related to management's risk assessment and should be at least partially satisfied through proper completion of risk assessment documentation in this toolset. Additional documentation resulting from audits and other monitoring activities, such as management action plans, management responses to audit findings, and six-month follow-ups should be applied during the risk assessment process and be maintained to demonstrate compliance with these requirements.

4. Management develops and maintains documentation of its internal control system. (paragraph 3.09)
5. Management documents in policies the internal control responsibilities of the organization. (paragraph 12.02)
6. Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify internal control issues. (paragraph 16.09)

Examples of documentation that may be used to meet requirements 4, 5, & 6 above include policies of accountability, procedural documents, continuity manuals, organization charts, job descriptions, code of ethics/conduct, performance evaluations, training records, control testing results, and management action plans.

A template for capturing management action plans is also included in the workbook with the forms. If a deficiency in the design or implementation of a particular principle or control activity is detected during any phase of the risk assessment process, a description of the deficiency and a management action plan including estimated completion date must be documented.

For additional guidance it is strongly encouraged that each user of these forms reviews the applicable sections of the 2014 GAO Green Book, which can be found at the link on page 1 and below.

