I. Audit Approach

This audit of IT Project Management will be approached from the perspective of the COSO (Committee Of Sponsoring Organizations of the Treadway Commission) integrated internal control framework that has been adopted by the Regents. Information for the audit program was also obtained as necessary from the Institute of Internal Auditor’s GTAG (Global Technology Audit Guide) #12 (*Auditing IT Projects*), the IT Governance Institute’s COBIT (Control OBjectives for Information and related Technology) framework—Process PO10 (*Manage Projects*), and the fourth edition of the Project Management Institute’s *Project Management Body of Knowledge* (Fourth Edition).

The COSO framework models internal control as a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

● Effectiveness and efficiency of operations.

● Reliability of financial reporting.

● Compliance with applicable laws and regulations.

The above objectives are one of three dimensions of internal control in the COSO framework. The other two dimensions are internal control elements (control environment, risk assessment, control activities, monitoring, and information and communication); and an entity’s units or activities. Within the framework, internal auditors are envisioned as having the role of evaluating the effectiveness of control systems and playing a monitoring role.

Based on COSO, for purposes of this audit IT Project Management is viewed as an organizational activity, the objectives of which are that (1) IT projects are operationally effective and use organizational resources efficiently; (2) IT project financial information is collected and processed in such a way that the reliability of overall financial reporting at the campus-, medical center-, or laboratory level is not adversely affected; and (3) IT projects adequately address compliance with laws and regulations as applicable.

Collectively, the sources referred to above identify risks associated with the three objectives just listed, as well as risk-mitigating best practices. Accordingly, this audit consists of two parts. The first is an overview and risk assessment. The overview’s purpose is to identify the existing audit population of IT projects, and, with respect to that population, to determine the extent to which risk-mitigating best practices are established. Based on this information, a judgment is then to be made as to the level of residual risk of project failure.

The outcome of the overview and risk assessment will determine the nature and extent of work in the second part, which is an optional (subject to auditor judgment) detailed evaluation.

**II. General Overview and Risk Assessment (required)**

1. Identify the population to be audited. Suggested criteria: those projects completed within the most recent two-year period that primarily involve acquisition, development, maintenance of, or change to, an electronic information system, and whose impact extends to an entire campus, medical center, or laboratory.
2. Use the template embedded below to help identify existing control practices with respect to the audit population as a whole, in comparison with best practice, and, based on this information, to record a judgment as to the level of residual risk of project failure generally. It is suggested that the template’s control content be shared with cognizant management as a basis for inquiry, in lieu of a traditional internal control questionnaire.



Subject to auditor judgment, if the results of the overview and risk assessment are enough to enable a dialog about recommendations and corrective action in agreement with management, or enable a conclusion that residual risk is low, further audit work need not be performed. On the other hand, if the results of the overview and risk assessment do not have this outcome, detailed evaluation should be performed.

**III. Detailed Evaluation (if deemed necessary)**

1. **Option 1: Further Control Verification**

If the overview and risk assessment indicated the presence of risk-mitigating best practices, but there remains some uncertainty as to the degree to which the asserted practices are actually operational, consider conducting further inquiry as necessary to conclusively determine their status. To conduct this inquiry, pick a sample of the control conditions in the overview and risk assessment template on which to focus this additional effort, and seek additional evidence of their operational status as circumstances warrant.

1. **Option 2: Testing of Individual IT Projects**

If the overview and risk assessment indicated control insufficiency, but there was not agreement with cognizant management about this insufficiency or about possible corrective action, consider detailed testing of individual IT projects. To conduct this testing, apply criteria from the GTAG matrix embedded below, as necessary, to a sample of the audit population of IT projects, to help determine the extent to which they:

1. achieved their objectives;
2. were concluded timely;
3. were concluded within their established budget; and
4. were concluded without adverse organizational or operational side-effects.

