KPMG

How to do a Green Book assessment of your internal controls

Your questions answered

March 2018

kpmg.com

At a time when state and local governments are being asked to do more with less, management may consider the task of assessing and upgrading internal controls to comply with federal guidelines as an administrative headache.

But as we noted in a recent thought leadership piece, Internal controls: Leading Practices for State and Local Government Organizations, using the Green Book as a framework for internal controls has become a leading practice. Indeed, an assessment and monitoring of your controls can be a valuable opportunity to identify:

— Enhance enterprise risk management efforts

— Redundant or out-of-date practices that can be streamlined

— Areas for use of innovative technologies, including the use of intelligent automation for routine tasks

— Leading practices that can be migrated across the organization

— Enhance accountability and transparency of the use of taxpayer funds.

Organizations that have adopted the Green Book, and those considering making the commitment to the leading practice, encounter some of the same questions to implementation, such as how to go about the process. Participants in our recent Webcast on Green Book implementation had a number of questions on that subject, and following, we provide some answers.

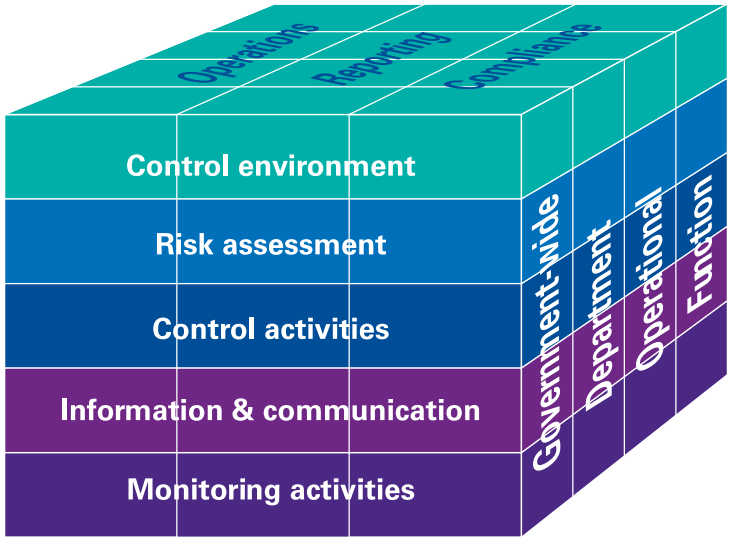
KPMG

What is the role of the internal auditors in a control assessment?

The internal auditor is one of the "three lines of defense" in effective risk management and control, following after operational management, and risk and compliance functions. In this capacity, the internal auditor assesses the controls that management has designed and implemented and tests those controls for operating effectiveness. The Internal Audit (IA) team can work collaboratively with management to help the organization remain on track with its control-related goals and objectives.

Organization board

Sets organization's objectives



Framework used to manage risk and control to accomplish objectives

First line of defense		Second line of defense	Third line of defense
Management controls	Internal control measures	Financial control	Internal audit
		Security	
		Risk management	
		Quality	
		Inspection	
		Compliance	

Organizational structure to execute risk and control duties

The IA team has visibility across the organization. Consequently, it brings significant value to the control documentation and assessment process by identifying leading practices in one department that others across the organization can leverage. It can also provide a fresh set of eyes on day-to-day operations, and—without compromising its objective—assist management in periodic efforts to rethink and refresh established processes and controls.

KPMG

Must all 17 principles included in the Green Book be in place to have an effective control system?

Yes. The effectiveness of an internal control system depends on the effective implementation of each of the 17 principles that make up the Green Book's 5 components of internal control—Control Environment (Principles 1–5), Risk Assessment (6–9), Control Activities (10–12), Information and Communication (13–15), and Monitoring (16–17).

In short, the 17 principles work together to create an effective control system. A lack of one of the principles can significantly affect the system as a whole. Example scenarios and potential impacts are outlined below.

- If an organization lacks the principles of **control environment** (foundation of an internal control system), the best-designed process controls may not likely be executed effectively.
- If an organization lacks the principles of **risk assessment**, the focus of the internal controls may not be on the areas that need to be controlled, reducing the cost effectiveness of efforts, and leaving other risk areas vulnerable.
- If an organization lacks the principles of **control activities** (policies and procedures), the organization may not operate effectively to respond to risks and meet business objectives.
- If an organization does not effectively manage **information and communication** regarding controls and processes, personnel may not know the expectations of the control, and how to execute them.
- Lastly, if an organization does not perform **monitoring activities** and follow-up on controls (assess quality over time, including issue resolution), employees can lose sight of control objectives and controls may not be effective or relevant.

As noted in Green Book section OV3.03, "To determine if an internal control system is effective, management assesses the design, implementation, and operating effectiveness of the 5 components and 17 principles. If a principle or component is not effective, or the components are not operating together in an integrated manner, then an internal control system cannot be effective."

What tools and templates are available to assist with the assessment?

Several sources provide useful assistance with the control assessment:

GAO implementation guidance (and plans) – The GAO developed its "Internal Control Management and Evaluation Tool" to provide guidance for the prior version of the Green Book. While the GAO is forming a task force to update it, the current guidance continues to offer useful insights. It can be found on the GAO Web site at https://www.gao.gov/products/GAO-01-1008G.

Peers – If you are getting started, your peers may be able to offer resources you can modify to meet your needs. Other good sources of information include legislation, policies, and templates created by many public sector organizations.

Consultants and tools – Professional service firms can help you develop and execute a control assessment and establish monitoring procedures. Additionally, software tools are available to facilitate the assessment. KPMG has developed a Web-based assessment tool, used as an engagement enabler, as part of our internal control assessment project management office.

What is the difference between a control assessment and enterprise risk management?

Enterprise risk management (ERM) is a leading-practice subset of a good internal control program. A formal ERM program includes a process to identify relevant organizational risks and categorize them along a matrix that considers the likelihood of occurrence and magnitude of impact.

The exercise is an important part of the internal control assessment, in keeping with Green Book principles 6–9:

6. "Management should define objectives clearly to enable the identification of risks and define risk tolerances.
7. "Management should identify, analyze, and respond to risks related to achieving the defined objectives.
8. "Management should consider the potential for fraud when identifying, analyzing, and responding to risks.
9. "Management should identify, analyze, and respond to significant changes that could impact the internal control system."

While many organizations do not have a formal ERM program, they must have processes in place to identify the risks an organization faces in achieving its objectives based on a reasonable level of risk tolerance. The organization mitigates those risks by developing appropriately controlled processes to execute the transactions necessary to meet the mission. Under OMB Circular A-123, the federal government requires its departments and agencies to perform annual enterprise risk assessment. While not applicable to nonfederal organizations, this requirement does represent a leading practice.

KPMG

How often should a "full assessment" be done?

In many cases, a full assessment of internal controls is done annually.

For public companies, Sarbanes-Oxley 404 requires that management sign off on controls over financial reporting and that an external auditor opine on the controls. For federal government departments and agencies, OMB Circular A-123 requires an annual internal control assessment and report as part of the annual financial report.

Public sector organizations do not have a statutory requirement to complete an annual assessment. However, the Uniform Guidance over federal grants, Section 200.303, does mandate that a recipient of federal funds must "establish and maintain effective internal control over the federal award…" and "evaluate and monitor the nonfederal entity's compliance with statute, regulations, and the terms and condition of federal awards."

Several state governments have adopted laws or regulations that require annual management reporting on the organization's assessment of controls, by department. To complete the certification, the organization must document the controls it has established (or updated from the prior year). Senior management has line managers self-assess the controls or implements a monitoring function (such as a quality assurance or internal audit group) to test that the controls are operating as designed.

Evaluations should be done by department or other unit. With the initial evaluation in place, during subsequent years, the organization can readily update in its annual evaluation any relevant changes in the policy, people, process, or technology that support the internal controls. Once documentation is complete, annual monitoring will allow management to meet the spirit of the uniform guidance, state policy, or law.

Why is it important to distinguish between a process and a control?

There are important differences between the two:

- **A process** is a series of steps to initiate, recognize, and disclose business transactions in a particular period. A process activity is where an **error can occur**. Key words: input, record, process, prepare, interface, and assess.
- **A control** is an activity that **mitigates processing risk** to an acceptable level (either directly or indirectly). A control activity is performed to **prevent or detect an error**. Key words: Review, authorize, compare, agree, reconcile, and validate.

When documenting and assessing processes, management should consider "what could go wrong" (WCGW) with the process. Appropriate control activities should be added to the workflow to mitigate the risk of WCGW to a level the organization deems acceptable. When controls are working effectively, the process will function and record transactions with minimal risk of error. An internal control assessment should provide an understanding of the process, but its focus is on how the controls should be designed to mitigate identified risks.

What opportunities can be identified if an internal control assessment is completed?

An effective internal control assessment can be much more than a compliance exercise. Indeed, such an assessment can help public sector organizations improve efficiency and effectiveness in the face of budget constraints and the significant "brain drain" that has begun with baby-boomer retirements.

New technology, for example, is providing public sector managers with an opportunity to evolve their organizations. The internal control assessment helps management identify gaps in the internal controls. Also, if it is performed with the right lens, the assessment can point to opportunities to add value:

9 **Areas where controls/processes are redundant and can be streamlined** – Many organizations add procedures and controls to mitigate newly identified risks (such as new regulations, new technology, identified noncompliance, or fraud). In some cases, the new procedures are layered over existing controls. Completing a control assessment allows management to step back, consider the cost/benefit of each incremental control, and then perform a controls rationalization to improve efficiency and effectiveness of the control environment.

9 **Areas that can benefit from implementation of innovative technologies** – With the growing use of intelligent automation, data analytics, and mobile technology, a control assessment can identify areas were routine manual processes could be replaced with a "bot" to free up people to perform more value-added tasks—resulting in the ability to devote more focus on the mission—critical objectives of the organization.

Call to action

As a result of the new Uniform Guidance, many state and local governments are now assessing their controls—both as a better practice for managing risk as well as an opportunity to rethink how they run their operations. They are using the Green Book framework to help them identify new opportunities and to evolve their organizations.

KPMG has helped many organizations find value when performing a controls evaluation. Details on how controls are functioning can indicate opportunities to improve processes and efficiency, reduce redundancy, use automation and standardization to lower control costs, strengthen risk mitigation (including protecting against fraud and cyber threats), and enhance service delivery.

The following are some actions to consider:

— **Get the internal auditors involved:** They understand internal controls and can jump-start your efforts.

— **Adopt an organization-wide management policy requiring that the assessment be completed:** Some organizations have even codified this into legislation.

— **Develop a structured process for documenting the control assessment:** A combination of questionnaires, flowcharts, and narratives is most effective.

— **Train your personnel:** All management personnel should understand the core concepts of good internal control.

— **Assess the risk of not achieving organizational objectives, and start the internal controls evaluation where the risk is highest:** Do not try to "boil the ocean"—make the effort structured and manageable.

— **Pause and reflect on the information you have gathered:** Analysis and creative thinking can lead you to the opportunities for improvements in operations.

— **Develop a plan to test the effectiveness of the design of the controls:** Most leading organizations are asking departmental managers to sign off on the effectiveness of controls for which they are responsible.

With an ever-changing environment that requires high-value activities to serve constituents, paired with tighter budgets, a Green Book assessment can provide organizations with critical information to manage risk and evaluate operational efficiency and effectiveness.

At KPMG, we join forces with our clients to help them realize an internal control assessment that moves beyond compliance. Let us know how we can help you.

KPMG

Contact us

For further information, please visit us online at **kpmg.com/infrastructure**, e-mail **infrastructure@kpmg.com**, or contact the following:

Joseph Seibert
Partner
T: 717-260-4608
E: jseibert@kpmg.com

Anthony Monaco
Partner
T: 212-872-6448
E: amonaco@kpmg.com

Rory Costello
Principal
T: 518-427-4826
E: rcostello@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia