Audit processes *take flight*

The updated COSO *Internal Control–Integrated Framework* is at the heart of Boeing's internal audit work.

Tim Boyle
Dennis Applegate

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) revised *Internal Control–Integrated Framework* offers internal audit departments an opportunity to take a fresh look at their processes for evaluating internal control. For the internal audit function at The Boeing Co., the release of the 2013 update has been the catalyst for adding more discipline and structure to its work.

The updated framework's most significant new development is that it codifies 17 guiding principles that articulate the concepts underlying the five control components described in the original version: control environment, risk assessment, control activities, information and communication, and monitoring activities. Moreover, it adds 77 explicit points of focus spread

across those principles to assist users in understanding the structure of a well-designed and effective internal control system. The framework now also requires organizations to use the principles to assess the effectiveness of internal control, although it allows management to determine the suitability of the points of focus.

COSO's revised internal control framework became its authoritative framework at the end of 2014. By 2015, Boeing Corporate Audit had updated its audit process, ensuring that its internal auditors consistently tested each control component and exercised sound judgment in determining whether all five components were *present* and *functioning*, and *operating together,* as articulated in the 2013 framework.

PRINCIPLES-BASED APPROACH

Boeing develops and executes a risk-based audit plan aligned with key business objectives. As a manufacturer of commercial and defense aerospace products, its audit plan primarily focuses on operational objectives such as the development of new airplane designs, management of suppliers—including procurement of major parts and assemblies such as engines and landing gear—and the production and testing of commercial and military aircraft. Such audits are generally not focused at the entity level, but rather on processes at the division, plant, product line, or functional level. For that reason, assessing all 17 principles on every audit would not add value for most audit clients. Instead, Boeing's internal auditors apply a subset of the COSO principles tailored to ensure that audit adds value on all engagements.

Audit management and staff brainstormed and documented the new COSO-based audit criteria using the principles and points of focus supporting the five COSO control components, but they adapted them to Boeing's environment (see "COSO Evaluation Considerations for Auditors" on page 38). This guidance has driven a consistent implementation of the 2013 framework, making it relevant and value-added to both auditors and clients, alike. Moreover, the criteria have compelled audit testing of all COSO control components for sufficiency, not just control activities. Auditors tend to focus the bulk of their control testing on the COSO control activities component because it is the component traditionally containing the preponderance of controls at the process-level. However, giving audit attention to all COSO components provides a more comprehensive evaluation of significant risk, better serving client management.

Because the 2013 framework cautions that the use of principles or points of focus are not meant to imply a checklist, Boeing's Corporate Audit staff is trained and empowered to exercise judgment in determining the nature and extent to which the criteria are applied. Yet they must take care to keep the focus always on inherent risk. The guidance on COSO principles and points of focus, coupled with the endorsed audit evidence, form the criteria that assist the company's internal auditors in assessing whether the components of internal control are present, functioning, and operating jointly.

AUDIT DOCUMENTATION

To back the new COSO-based approach, Boeing Corporate Audit developed a condensed and integrated audit template for documenting all relevant facts and data used to evaluate each COSO control component. It includes the guidance from the COSO Evaluation Considerations and requires auditors to document what was evaluated in the control design assessment phase and what was tested in the operational assessment phase, including the conclusions reached for each component. It also mirrors certain aspects of the traditional risk and control matrix that should be familiar to most internal auditors. This "extended risk control matrix" (E-RCM) is a required audit workpaper for each process objective in Boeing's internal audit protocol and provides audit management a point of departure in due diligence reviews of the audit work performed, a quality assurance step designed to comply with IIA Standard 1311: Internal Assessments.

In the preliminary survey phase of the audit, the E-RCM serves two key purposes. First, it shows the alignment of process controls to the related COSO control component. Second, it allows the internal auditor to document potential control gaps and to indicate whether the alignment of controls provides sufficient risk coverage.

In the fieldwork phase, auditors document the testing of the defined controls for design and operating effectiveness in separate columns of the E-RCM. Such documentation provides support for the auditor's opinion on the discrete controls and how those controls may or may not support the components as being present, functioning, and operating together.

Moreover, every audit requires a detailed process flowchart. Confirmed with client management, the flowchart details the movement of activities and documents through the process, and identifies key control points requiring audit examination. Many audit professionals use process flowcharts to define and document their understanding of the audit subject. The same purpose is served in Boeing's COSO-based audit process, though the process flowchart has taken on an extra dimension as the initial basis for the E-RCM.

96% of companies reviewed in fiscal year 2015 have adopted the 2013 COSO *Internal Control–Integrated Framework*, according to an analysis by Audit Analytics and Protiviti.

The key elements of the revised audit process, as reflected in the E-RCM, are:

- *Process objective.* Derived from relevant company policies and procedures, industry standards, or other business goals and confirmed with client management before an audit begins.
- *COSO components.* Each discrete control to be assessed as part of the audit is grouped with the component to which it is most closely aligned. The results of the control assessment are then used to support the evaluation if that component is present and functioning in support of the process objective. If no specific controls are associated with a component, then the component is still evaluated through inquiry, observation, and inspection, as needed.
- *Inherent risk.* Documents negative events and their effects on achieving the predetermined process objective in the absence of management controls.
- *Controls.* Describe the attributes of each risk-mitigating control, including *who* is responsible for the control, *how* and *when* control execution is accomplished, *what* is involved in executing the control, and *why* it is important.
- *Control design assessment.* Documents how each control was assessed for design effectiveness, the results of that testing, which of the various controls are key, and whether those controls are present to achieve the objective. This control testing, along with the process-level evaluation, supports the overall opinion on whether the COSO components are present and working together.
- *Operating effectiveness testing.* Documents the results of audit tests of control operation, emphasizing the use of audit sampling techniques to determine whether the controls are functioning as designed.
- *Conclusion.* Summarizes the auditor's determination of whether each of the five components is present, functioning, and operating together as a unit to provide reasonable assurance of achieving process objectives.

The updated audit process provided an opportunity for increased discipline in defining processes, risks, and controls.

THREE KEY ELEMENTS

Although the elements of business processes, risks, and controls have been a focus of Boeing's internal audit work for many years, the updated audit process provided an opportunity for increased discipline in the definition and alignment of these three key elements.

Process Objectives In Boeing's revised audit process, auditors issue an opinion to client management on whether the COSO control components are present, functioning, and operating together in support of the stated process objective, pursuant to the 2013 framework. Typically, a process objective will fall entirely within operations, reporting, or compliance—the basic objective categories defined by COSO—but occasionally it may cover more than one COSO objective.

The E-RCM documentation supports each assessment by component and provides a clear line of sight from

continued on page 40

TO COMMENT on this article,
EMAIL the authors at tim.boyle@theiia.org

COSO EVALUATION CONSIDERATIONS FOR AUDITORS

CONTROL ENVIRONMENT

1 Are the responsibilities, accountabilities, and authorities (RAA) established and communicated effectively through policies, procedures, or other methods to support process and control objectives?

- Are control performers' responsibilities aligned with authority or accountability?
- Are organizational responsibilities identified (e.g., charter and structure) and people assigned to achieve the process objectives and key deliverables?
- Is there segregation of duties to mitigate misrepresentation or misstatement of operations (fraud risk)?

Potential Audit Evidence to Support Conclusions
Inspect organizational charts/charters and confirm that current job responsibilities are aligned with relevant process objectives.

2 Do control performers have sufficient competencies to execute controls?

- Do they understand the risk and objective of the control?
- Does the control performer have the experience/training necessary to execute the control?

Potential Audit Evidence to Support Conclusions
Evaluate results of control testing (as applicable) where competence is an attribute.

3 Are management actions and priorities consistent with stated objectives, RAA, and Boeing values?

Potential Audit Evidence to Support Conclusions
Evaluate whether management actions align with supporting process objectives (i.e., demonstrated allocation of resources, priorities are managed to stated objectives, and corrective actions are taken).

RISK ASSESSMENT

1 Is a risk assessment occurring on a regular basis for the process? It could be formal or informal, but it should be happening in some form by management.

Potential Audit Evidence to Support Conclusions
Attend meetings to observe where risks are identified, monitored, and actions are taken. Are stakeholders represented and is the frequency adequate to help with risk mitigation?

2 Are process objectives defined specifically enough to support identification of inherent risk events?

Potential Audit Evidence to Support Conclusions
Inspect process objective definitions to evaluate whether objectives are stated specifically enough to support risk identification (this may not be documented, so use inquiry as needed).

3 Are inherent risk events identified and assessed?

- Are internal or external business changes (e.g., regulatory, funding, market, business growth or reduction, and system changes) considered within the risk assessment?
- Is the risk assessment occurring frequently enough to capture these changes?
- Have key stakeholders been identified and are they involved in the risk assessment?
- Are nonconformances or negative trends captured and evaluated for inclusion in the risk assessment?
- Are potential fraud risks (financial or nonfinancial) identified and evaluated (e.g., a nonfinancial fraud risk such as metrics that are intentionally misrepresented to hide poor performance or risk (reported as yellow; when they are red))?
- Are risk tolerances established, (e.g., a 2 percent error rate for manufacturing defects).

Potential Audit Evidence to Support Conclusions
Inspect identified risks for completeness of events (this may not be documented, so use inquiry as needed). Inspect metrics for negative trends and inclusion in risk assessment for systemic issues.

4 Has management determined appropriate risk response (i.e., accept, avoid, reduce, or share)? (See Control Activities.)

Potential Audit Evidence to Support Conclusions
Inspect control implementation as documented in policies and procedures, business process instructions, desk instructions, or other methods to evaluate whether identified risks are adequately responded to with controls.

COSO-based internal control systems can meet "the challenges of an ever-changing business and regulatory environment," notes Adding Value With COSO from the Internal Audit Foundation.

CONTROL ACTIVITIES

1 Are the controls designed and operating effectively to achieve their objectives, to mitigate the risks, and support the process objective?

» Control testing of attributes using statistically relevant samples will be the primary way to evaluate control activities.

Potential Audit Evidence to Support Conclusions

Control test results will be the most influential data for conclusion.

2 Based on the evaluation of risk events inherent to the process, have corresponding controls been identified? (See Risk Assessment.)

» Are there enough controls developed and implemented to mitigate the risks in the process (i.e., preventive, detective, manual, general computing controls, and IT dependent as needed)?

Potential Audit Evidence to Support Conclusions

Inspect process guidance where controls are defined, such as relevant command media, desktop procedures, manuals, and monitoring. Do they align with identified risks?

3 Are controls defined, documented, and communicated (e.g., command media, desktop procedures, manuals, and training)? (See Information & Communication.)

Potential Audit Evidence to Support Conclusions

Inspect control documentation and communication to control performers for sufficiency. Factors to consider for level of documentation include complexity of controls, significance of risks, number of control performers, and turnover expected. Lack of documentation may or may not be a deficiency.

INFORMATION & COMMUNICATION

1 For affected stakeholders, is information identified, validated, documented, communicated, and reviewed to achieve process objectives such that control performers can execute consistently (i.e., process steps, process RAA, control RAA, control definitions and objectives, changes to relevant policies, procedures, risks, and new initiatives)? (See Monitoring Activities.)

» Is documentation sufficient to match the level of risk and complexity of control?

» Is there data identified to support monitoring of control performance?

» Are there open channels of communication both top-down and bottom-up?

Potential Audit Evidence to Support Conclusions

Inspect information and communication of other relevant information (i.e., business/process objective statements, command media, change notifications, and metrics) and assess whether it is disseminated to relevant stakeholders (i.e., control performers, process owners, and management/customers/suppliers). (See Control Environment.)

» *Inspect process documentation to evaluate adequacy to support consistent execution by the control performers. (See Control Activities.)*

» *Inspect controls for associated information used to monitor and evaluate whether there is sufficient and reliable information and communication to identify failures timely.*

MONITORING ACTIVITIES

1 Does effective monitoring of the internal controls of the process exist?

» Are metrics in alignment with objectives, risk tolerance levels, and controls?

» Are out-of-tolerance conditions consistently identified (i.e., red and yellow criteria; or methods of effectiveness identified)?

» Are corrective/preventive actions identified, approved, and tracked to completion?

Potential Audit Evidence to Support Conclusions

Inspect metrics in use to evaluate whether they are aligned to the key objectives and risks, and that there are clear criteria for identifying unacceptable conditions.

2 Are metrics validated and communicated to relevant stakeholders? (See Information & Communication.)

Potential Audit Evidence to Support Conclusions

Inquire and inspect how metrics are validated and communicated to stakeholders.

VISIT InternalAuditor.org to view the extended risk control matrix, risk definitions, and control model used by Boeing's Corporate Audit department.

continued from page 37

the process objective through the risks, controls, tests performed, and data used for the final assessment. The structured nature of the revised audit process also helps ensure that the auditor judgment exercised in rendering an opinion about the control components is informed by relevant audit facts and data. Concentrating an audit on process-specific objectives improves auditor focus and efficiency, enhances client understanding, and helps guard against scope creep. More importantly, it avoids overstating the final audit opinion, limiting it to the scope of the process objective and what was actually tested.

Assessment of Inherent Risk The 2013 COSO framework contains a more detailed conceptual analysis of inherent risk, control risk, and risk tolerance than the prior version. In response to this new COSO emphasis, Boeing Corporate Audit has increased its focus on auditor understanding of risk management concepts and the appropriate exercise of auditor judgment when determining the nature and extent of inherent risk. In rolling out the COSO-based audit process, Boeing further emphasized not only the need to identify inherent risk in all audits but to avoid conflating this risk with control risk, a distinction that the new COSO framework also has addressed.

Boeing uses a COSO-inspired risk model in auditor training. The model contains abbreviated versions of the COSO definitions for inherent, control, and residual risks, and a simple equation to show the corresponding risk relationships to client management. Auditor understanding of client management's risk tolerance also has assumed greater importance in the new COSO framework, and that requirement has been built into the risk assessment procedure. Despite their subjectivity, these risk concepts become meaningful to the audit client when modeled into a heat map.

The Control Model To ensure consistency in ascribing a particular control to a given component, Boeing Corporate Audit established a control model based on the concepts contained in the 2013 COSO framework. The control model defines 28 specific types of controls segmented by COSO components that may be present in each process, irrespective of the process objective. Some of these control types may cover more than one component. For example, "review performance metrics" may address the control activities component if the metrics pertain to management supervision or address the monitoring component if the metrics pertain to reviews of the internal control system. These criteria have helped internal auditors identify relevant controls and classify them by the control component prescribed in the model. This has resulted in more consistent control definition and COSO alignment.

AUDITOR OPINIONS

Once the audit and supporting E-RCM documentation have been completed and approved, Boeing Corporate Audit summarizes the evaluation of each control component and issues to the client an overall opinion about the health of the internal control system governing the process. Three kinds of opinions are possible:

- The internal control components were determined to be present and functioning, even though some low-impact audit findings may be present.
- The internal control components were determined to be present but not functioning.
- The internal control components were determined to not be present.

Each deficiency is documented in a finding that then requires a corrective action by management. The rationale for any adverse opinion and the impact of significant process errors or omissions are detailed in the accompanying audit report.

TANGIBLE RESULTS

Since adopting this model with an emphasis on inherent risk, Boeing's internal auditors have increasingly targeted control design improvements for management attention, resulting in a 61 percent increase in the number of audit findings related to control design. Such findings tend to provide more value to audit clients because they improve the quality of the overall internal control system rather than improve the execution of specific controls within a system that is poorly designed.

The documented process improvements at Boeing support the proposition that COSO-based auditing yields an effective audit result. Specifically, testing all five COSO control components and related principles using a consistent baseline of COSO criteria and control types provides a solid foundation for determining the level of assurance provided for the objectives being evaluated.

Adopting a COSO-based approach to internal auditing has aligned the Boeing Corporate Audit process with a key professional standard. While the path to adoption is not easily navigated, internal audit departments willing to make the journey will be rewarded by more thorough audit coverage. ia

TIM BOYLE, CIA, PE, *is senior audit manager at The Boeing Co. in Seattle.*
DENNIS APPLEGATE, CIA, CPA, CMA, CFE, *is an adjunct professor at Seattle University.*