ARMICS Update – What is new in internal control?

COSO's Internal Control – Integrated Framework (2013)

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) updated their Internal Control – Integrated Framework in May 2013. While the original framework remains fundamentally sound and broadly accepted in the workplace, the COSO Board recognizes there have been many changes in business and operating environments over the years. For example, expectations of governance oversight have increased; risk and risk-based approaches now receive greater attention; technology has evolved dramatically; and the demands and complexities in laws, regulations and standards have increased. The COSO Board's goal in updating the original framework is to formalize more explicitly the principles embedded in the original framework.

The 2013 Framework has several important changes, seven of which are summarized below. The quotations on the seven changes are taken from Protiviti's publication, *The Updated COSO Internal Control Framework, Frequently Asked Questions, Second Edition*.

First, the 2013 Framework codifies principles that support the five components of internal control. "While the 1992 version implicitly reflected the core principles of internal control, the 2013 version explicitly states 17 principles representing fundamental concepts associated with each of the five components of internal control."

Second, the 2013 Framework clarifies the role of objective-setting in internal control. "The 1992 framework from COSO stated that objective-setting was a management process, and that having objectives was a pre-condition to internal control. While the New Framework preserves that conceptual view, it moves the primary discussion of the concept from the chapter on risk assessment to the second chapter to emphasize the point that objective - setting is not part of internal control."

Third, the 2013 Framework reflects the increased relevance of technology. "Technologies have evolved from large stand-alone mainframe environments that process batches of transactions to highly sophisticated, decentralized and mobile applications involving multiple real-time activities that cut across myriad systems, organizations and processes. More sophisticated technology can impact how all components of internal control are implemented."

Fourth, the 2013 Framework incorporates an enhanced discussion of governance concepts. "These concepts relate primarily to the board of directors, as well as subcommittees of the board, including audit committees, compensation committees and governance committees. The key message is that board oversight is vital to effective internal control."

Fifth, the 2013 Framework expands the reporting category of objectives.
There are four types of reporting: financial – internal and external, and non-financial – internal and external. The reporting category now focuses on other types of reporting than just financial reporting.

Sixth, the 2013 Framework enhances consideration of anti-fraud expectations. "The 1992 framework considered fraud, although the discussion of anti-fraud expectations and the relationship between fraud and internal control were less prominent. The 2013 version contains considerably more discussion on fraud and also considers the potential causes of fraud as a separate principle of internal control."

Seventh, the 2013 Framework increases the focus on non-financial reporting objectives. "This expanded focus on operations and compliance and non-financial reporting objectives has provided more robust guidance in these areas."

"The above changes, while important, in no way constitute a complete overhaul." The New Framework is similar in substance and all material aspects to the 1992 framework. **The most important change is the "explicit articulation of the 17 principles representing the fundamental concepts associated with each component of internal control."**

The 17 principles are listed below and grouped according to the applicable control component:

Control Environment

1. The organization demonstrates a commitment to integrity and ethical values.

2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

4. The organization demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives.

5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

9. The organization identifies and assesses changes that could significantly impact the system of internal control.

Control Activities

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

11. The organization selects and develops general control activities over technology to support the achievement of objectives.

12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information and Communication

13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.

14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.

Monitoring Activities

16. The organization selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Agency Risk Management and Internal Control Standards (ARMICS) Updated

The ARMICS standards were updated in August 2015 with revisions to pages: 5, 12, 21, 27, 30 and 37. Changes include:

- ARMICS was updated to include reference to the 2013 revision of the COSO Internal Control – Integrated Framework. (Page 5)

- ARMICS states that, "While each state employee has personal internal control responsibility, the agency head holds ultimate responsibility and must assume ownership for internal control. Other agency executives and managers must support the agency's internal control philosophy, promote compliance, and maintain control within their areas of responsibility." In order to explicitly meet COSO principle No. 5, agencies can include internal control responsibilities in Employee Work Profiles (EWPs), policies, procedures, and their Code of Ethics. (Page 12)

- The ARMICS minimum requirements were modified so that the risk of fraud must be included in the agency-level risk assessment. The transaction-level assessments of each agency fiscal process must also include the risk of fraud. Fraud originating inside an agency, as well as fraud perpetrated by individuals outside of the agency, should be considered. (Page 21)

- The ARMICS minimum requirements now include that agencies using another agency (Service Provider Agency) or a Third-party Service Provider to perform significant processes or functions, must obtain internal control assurance from that provider. See CAPP Topic No. 10305, *Internal Control*, for more guidance. (Page 27)

- Clarification that the checklists and questionnaires found in Appendix A and Appendix A-1 of the ARMICS standards document do not substitute for 1) verification of the existence of a control, or 2) testing in order to determine if a control is functioning properly. (Page 37)

- Lastly, while the "stages" of ARMICS were used to describe the phases of a complete internal control assessment, references to Stage 1, Stage 2 and Stage 3 have been removed from the standards document. ARMICS is an annual and perpetual requirement for all agencies, which includes the agency-level assessment, transaction-level assessment and any required corrective action plans.

How does ARMICS compare to the new COSO Internal Control Framework?

The Comptroller's ARMICS standards are based primarily on COSO's 1992 Internal Control Framework, yet reflect some content from COSO's 2004 Enterprise Risk Management Framework.

DOA cross-walked the 17 COSO principles from the 2013 update to the ARMICS standards and found that the principles were articulated within the ARMICS documentation. A full comparison of these 17 principles to the requirements and instructions contained in ARMICS can be found in the *ARMICS Crosswalk to COSO* document on DOA's website.

What else is new??

ARMICS Checklist

DOA reviews ARMICS documentation to determine if the minimum requirements according to the Agency Risk Management and Internal Control Standards have been met. These requirements can be found on pages 18, 21, 27, 31, and 35 of the standards.
http://www.doa.virginia.gov/Admin_Services/ARMICS/ARMICS_Standards.pdf

DOA has developed an ARMICS review checklist that agencies can use to see if they meet the minimum requirements of ARMICS. This is on the DOA ARMICS webpage:
http://www.doa.virginia.gov/Admin_Services/ARMICS/ARMICS_Review_Checklist_Agency.pdf

Revised Process Template

DOA has also included a revised template for documenting significant processes, risks and controls on the website.

Update to CAPP Topic No. 10305 (Both CARS and Cardinal versions)

- CAPP Topic No. 10305, *Internal Control*, has been updated to include an agency statement for those who have not implemented ARMICS or have not done annual testing of controls. **Agencies who have not complied with ARMICS cannot certify to the Comptroller.**

- Also included in the CAPP Topic No. 10305 update is a Certification of Internal Control for third-party providers who are not agencies of the Commonwealth.

- New guidance for Corrective Action Plans is provided as well, which includes new preparation and submission requirements. The status of all Corrective Action Plans will be reported in the Quarterly Report.