COSO

Committee of Sponsoring Organizations of the Treadway Commission

Governance and Internal Control

COSO INTERNAL CONTROL – INTEGRATED FRAMEWORK:

An Implementation Guide for the Healthcare Provider Industry

By

Crowe

Annette Schandl MSIB, CPA | Philip L. Foster MBA, ARe, ARM, AIC, CPCU

January 2019

Authors

Annette Schandl
Managing Director
Crowe

Philip L. Foster
Senior Vice President
CommonSpirit Health

COSO Board Members

Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by the following organizations:

American Accounting Association (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

COSO
Committee of Sponsoring Organizations
of the Treadway Commission

coso.org

Governance and Internal Control

COSO INTERNAL CONTROL – INTEGRATED FRAMEWORK:

An Implementation Guide for the Healthcare Provider Industry

Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Commission

January 2019

Contents

Introduction

This guide is the result of a collaboration of the Committee of Sponsoring Organizations of the Treadway Commission (COSO), Crowe, and CommonSpirit Health. Its purpose is to introduce nonpublic healthcare organizations to the COSO 2013 revised "Internal Control – Integrated Framework" (*2013 Framework*) and provide implementation guidance to help strengthen and enhance their overall governance and internal control structures. The enhancement is essential as healthcare organizations have evolved from stand-alone community-based acute care hospitals to regional and national systems providing the full continuum of healthcare. Not only has size increased exponentially but so has the complexity of organizations and the environments in which they operate. Debt structure, IT infrastructure and applications, health insurance interfaces, increased provider employment, life-dependent processes, and additional state and federal regulations all have added complexity and risk for healthcare leaders to address and governance functions to oversee. Effective internal control is vital for both of these stakeholders in order to successfully weather the ever-changing healthcare environment.

Executive summary

In May 2013, COSO released a revised "Internal Control – Integrated Framework," which replaced the original version developed in 1992. The original framework formally defined internal control and contained relevant and helpful guidance. In 2002, the *Sarbanes-Oxley Act* (SOX) was established; it mandates that U.S. listed companies report on the effectiveness of their internal control over financial reporting (ICFR) using a suitable framework and in some cases also requires separate audit of ICFR. Subsequently, most U.S. listed companies have chosen the framework* as their basis for compliance with Section 404 of SOX. Many countries including Japan, China, and South Korea have modeled some financial reporting legislation and other requirements related to internal control using concepts in the 1992 and 2013 versions of the framework. Furthermore, many organizations around the world have voluntarily used the framework to help them create, develop, mature, and continuously improve their systems of internal control beyond just financial reporting.

Organizations operating in the healthcare sector, regardless of size, maturity, or form of ownership, have unique challenges and opportunities relating to the design and operation of internal control structure. Challenges, generally associated with implementation of 2010's *Patient Protection and Affordable Care Act,* commonly called the *Affordable Care Act* (ACA), have placed considerable pressure on organizations – especially in the areas of regulatory compliance, healthcare delivery and associated patient outcomes, accessibility, cost management, technology, and information security. The ACA represents the most significant regulatory overhaul of the U.S. healthcare system since the passage of Medicare and Medicaid in 1965. Under the act, hospital systems and physicians need to transform healthcare delivery and focus on improved patient health outcomes, lower costs, and improved accessibility.

To make matters more challenging, the ACA has been under scrutiny since inception, resulting in potential changes to the act depending on the makeup of the U.S. Congress as well as its focus and intent. This leaves healthcare organizations, healthcare insurers, states, and small businesses in a state of ambiguity about how exactly a repeal of or change to the ACA would affect them. Those organizations have no choice but to run their business as usual with the expectation that regulatory oversight of the healthcare industry will continue to be very high. Therefore, due to the ever-increasing complexity of legal requirements and the associated challenges, leaders from across the healthcare industry increasingly are asking about the possible benefits of *2013 Framework* adoption. This is in spite of an absence of requirements and obligations for healthcare entities to formally report on internal control, unless those organizations are listed on a U.S. stock exchange or subject to SOX because of public debt. While most U.S. public companies use the *2013 framework,* it is important to note that it is designed to apply to all types of entities, including private, nonprofit, and governmental entities.

This implementation guide – which may be especially helpful to those who have only limited experience with implementing the *2013 Framework* – will explore how healthcare organizations can apply the *2013 Framework* to evaluate their existing internal control structure, implement controls to assist in mitigating significant risks, and optimize the effectiveness of their control environments, governance, compliance, management, and assurance functions. Providers of acute care such as single-facility hospitals and large, multifacility health systems can use the guide, and it also is applicable to providers in an ambulatory setting and to organizations operating in the broader healthcare space.

Benefits of *2013 Framework* implementation in healthcare

As mentioned earlier, healthcare has become increasingly complex, which in turn results in increased likelihood and greater impact of associated risks. For example, organizations are constantly under pressure to meet the requirements imposed by the ACA, providing continuous training to their medical staff to ensure consistent and appropriate patient care followed by proper clinical documentation. The implementation of electronic health record (EHR) systems over the past several years at most health organizations has added further to the pressure on clinicians, support staff, and management to show improvement in care and efficiency and provide evidence of proper implementation to the government in order to maximize appropriate reimbursement. Failure to meet certain ACA requirements can result in potential reductions in Medicare and Medicaid reimbursement and can be a significant financial hardship for many hospital systems and healthcare providers. With the implementation of the ACA, there is an intentional move away from fee for service to reimbursement based on quality, value, and outcomes. The resulting increased scrutiny of patient billing and clinical documentation, the constant loom of potential IT patient data breaches, and physician and nursing shortages in many parts of the country may cause many organizations to struggle with maintaining day-to-day control of business operations. Collectively, these challenges, without internal control, may threaten a healthcare organization's ability to achieve its operational, compliance, and reporting objectives.

Strong internal control can help mitigate many of the risks associated with such complex pressures. According to COSO, the implementation of the *2013 Framework* "is expected to help organizations design and implement internal control in light of many changes in business and operating environments since the issuance of the original *1992 Framework*, broaden the application of internal control in addressing operations and reporting objectives, and clarify the requirements for determining what constitutes effective internal control."[1]

Bill Watts, a risk consulting partner with Crowe, noted, "COSO provides a road map to building a fundamental foundation of internal control to ensure that the risks an organization takes are monitored and mitigated through sound business decisions." Healthcare organizations that formally adopt the *2013 Framework* may achieve numerous benefits, including but not limited to the following:

- Prioritizing and bringing focus to managing processes that are most likely to have an impact on accomplishing significant goals and objectives
- Re-evaluating and strengthening the internal control structure, particularly at the entity level
- Identifying internal control gaps for remediation Improving financial reporting assurance
- Identifying opportunities to streamline controls and reduce inefficiencies and redundancies
- Assessing important compliance areas such as the reduction and deterrence of fraud or the protection of health information
- Advancing and aligning enterprise risk management (ERM) with internal control
- Improving corporate governance
- Providing the ability to integrate compliance requirements into internal control
- Improving healthcare delivery through uniform internal control application
- Allowing relevant service providers (e.g., external auditors, partners) to increase reliance on the entity's internal control
- Improving the organization's ability to manage change
- Addressing constant cybersecurity threats

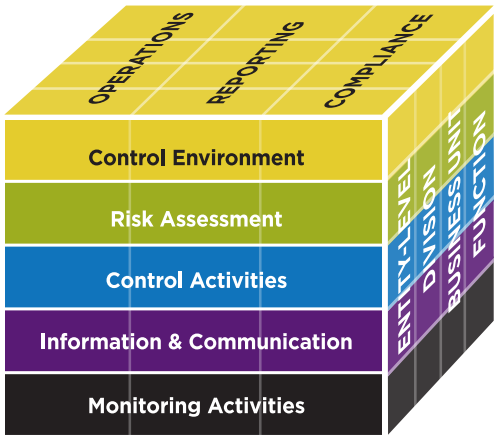
Many healthcare organizations already have elements of either formal or informal internal control structures in place. For example, most hospital systems have written policies and procedures pertaining to the processes in the areas of financial close, accounts payable, supply chain, and human resources. But often policies and procedures may be out of compliance with recent changes in federal rules and regulations, especially in areas relating to the revenue cycle, since the main focus of many hospital systems or physician practices has been to get systems functional with little to no disruption in patient care. Healthcare organizations experience issues with system access, system integrity, clinical documentation, coding, and billing, all of which may result in potential noncompliance with federal and state regulations – and costly mistakes. Formally adopting the *2013 Framework* facilitates an increased understanding of the internal control in existence, after which time improvements can be addressed in a prioritized fashion, resulting in reduced risk for all stakeholders. Watts added, "Healthcare organizations must review their control environment to confirm proper controls are in place to ensure effective and efficient operations, proper financial reporting, and compliance exist and that their control environment supports the obtainment of the organization's mission and strategy, and COSO provides the direction to do this."

The COSO *2013 Framework*

The *2013 Framework* focuses on five integrated components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities (see Exhibit 1). The updated *2013 Framework*:

- Clarifies the application of the *2013 Framework* in today's environment with the various business models, technology, and related risks
- Codifies criteria that can be used in developing and evaluating the effectiveness of systems of internal control – making explicit 17 principles, each with points of focus (see Exhibit 2)
- Expands reporting objectives to support internal, financial and nonfinancial reporting, and operational and compliance objectives
- Emphasizes the need for judgment in evaluating whether a company achieves effective internal control
  Focuses on accountability for internal control throughout the organization starting at the board level and senior management
- Explicitly considers IT controls and identifies the need for fraud risk consideration not limited to financial statements but also within compliance and operations

Exhibit 1. **The COSO Cube**



Components of internal control

The **control environment** describes a set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. According to the Institute of Internal Auditors (IIA), a control environment is the foundation on which an effective system of internal control is built and operated in an organization that strives to 1) achieve its strategic objectives, 2) provide reliable financial reporting to internal and external stakeholders, 3) operate its business efficiently and effectively, 4) comply with all applicable laws and regulations, and 5) safeguard its assets.

The **risk assessment** forms the basis for determining how risks will be managed. A risk is defined as the possibility that an event will occur and adversely affect the achievement of organizational objectives. Risk assessment requires management to consider the impact of possible changes in the internal and external environment and to potentially take action to manage the impact.

Control activities are actions (generally described in policies, procedures, and standards) that help management mitigate risks in order to ensure the achievement of objectives. Control activities may be preventive or detective in nature and may be performed at all levels of the organization.

Information is obtained or generated by management from both internal and external sources in order to support internal control components. **Communication** based on internal and external sources is used to disseminate important information throughout and outside of the organization, as needed to respond to and support meeting requirements and expectations. The internal communication of information throughout an organization also allows senior management to demonstrate to employees that control activities should be taken seriously.

Monitoring activities are periodic or ongoing evaluations to verify that each of the five components of internal control, including the controls that affect the principles within each component, are present and functioning.
around their products.

The *2013 Framework* is a flexible, reliable, and cost-effective approach to the design and evaluation of internal control systems for organizations looking to achieve operational, compliance, and reporting objectives. The *2013 Framework* can be applied regardless of organization size or type: public companies, privately held companies, not-for-profit entities, and governmental entities.[2]

Exhibit 2. **5 components and 17 principles of internal control**

5 components	17 principles
Control environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority, and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability.
Risk assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys control activities through policies and procedures
Information and communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Source: Adapted from the COSO "Internal Control – Integrated Framework"

Approaching the *2013 Framework* implementation

Before launching into the next sections, it is important to briefly examine some basic concepts and why those concepts are such an integral part of the *2013 Framework* implementation. COSO defines 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 relating to operations, reporting, and compliance." COSO provides further characterization of the objectives, which allow organizations to focus on different aspects of internal control: "*Operational objectives* pertain to effectiveness and efficiency of the entity's operations, including operational and financial performance goals, and safeguarding assets against loss. *Reporting objectives* pertain to internal and external financial and nonfinancial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity's policies. *Compliance objectives* pertain to adherence to laws and regulations to which the entity is subject."[3]

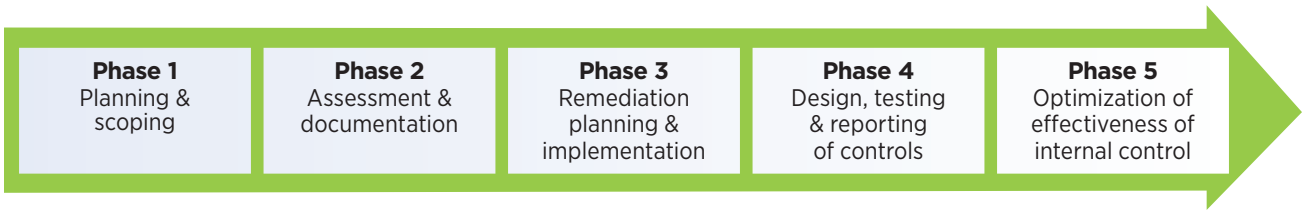
The hospital system has to comply with a significant number of laws and regulations before the patient even steps through its doors, while the patient is being cared for, and after the patient leaves when billing is performed. If any of those operational processes is not working properly, there will be a financial impact to the organization because of the inability to obtain reimbursement for the services rendered. Given the importance of internal controls, their design and execution (or lack thereof) can greatly affect the various objectives and strategies of an organization, ultimately affecting its success.

As an example of how those objectives apply to a process within a healthcare organization and how important it is to set objectives, let's use the revenue cycle. Typically, the revenue cycle is considered a high-risk area to an organization, and it requires many controls throughout the process. As a patient receives services in a healthcare setting, numerous departments are involved and necessitate continuous coordination and oversight. In addition to providing appropriate medical care, the process includes obtaining payment information (in the form of payment, insurance verification, or other means) from the patient, accurately coding and billing for the services rendered, and applying payments received to the patient account. Timely and detailed medical documentation by the medical staff is imperative. Consideration also needs to be given to the various IT systems (EHR, billing, etc.) that are used throughout the process. If these processes are not designed and implemented effectively, the healthcare organization may not achieve its operational, compliance, and reporting objectives within the revenue cycle.

Therefore, an organization's stakeholders play an important role in implementing the *2013 Framework*. For example, senior management and members of the board of directors should generally understand the *2013 Framework* and its implementation benefits, costs, and approach. These parties may already have a broad understanding of the necessity for an effective internal control system, and some may perform or support internal controls as a part of their daily routine. It is possible, however, that there may not be a full understanding of what is essential to implement the *2013 Framework*. This can be resolved through proper communication, training, and integration as well as a strong, supportive tone at the top, which are all elements imbedded within the *2013 Framework*.

Once awareness among the most senior leaders is established, the organization needs to formulate an overall plan for implementation, including mechanisms for gaining support throughout the organization. An implementation team should be staffed with individuals who have expertise in internal control and a strong working knowledge of the organization to minimize the learning curve. The implementation team should first spend time developing a project implementation plan, including plans for assessing, designing, implementing, and maintaining systems of internal control. The approach that follows (Exhibit 3) is one of many different ways the *2013 Framework* can be implemented within a healthcare organization.

Exhibit 3. **An approach to implementing the *2013 Framework***



Phase 1: Planning and scoping

Orientation

As mentioned earlier, it is important that executive management and the board are in full support of the implementation. Messaging and strong tone from the top will increase the likelihood of full cooperation throughout the organization. Note that the implementation usually requires additional resources – or at least existing resources such as employees who can dedicate a good portion of their time to the project. Once the implementation team is established, the team needs to gain a strong understanding of the *2013 Framework*, including the five components, the 17 principles, and the associated points of focus.

Given the current environment in many larger healthcare organizations that have gone through multiple mergers and acquisitions in recent years in order to increase performance and decrease costs, strengthening the current internal control environment in order to successfully handle the growth and complexity of the larger organization could be a significant driver in implementing the *2013 Framework*. Because of competing priorities, the board may want to delegate authority to a committee (e.g., an audit and compliance committee [A&CC]) to oversee the implementation process. The A&CC and management can then select a management function such as internal control or ERM to oversee the implementation efforts. Internal audit may assist the responsible function by providing advice and input based on their overall knowledge of the organizational internal control structure and areas of risk. Furthermore, the assistance of outside consultants could provide additional expertise and initial and continuous support.

Healthcare organizations also may find it necessary to use leaders and staff from within the accounting department, as those individuals may have broad familiarity with the entity's organizational structure and key process areas. It is most important to identify an ownership department that has deep, broad knowledge of how work is conducted within the organization. The ultimate selection will vary by organization, but it is also important to understand that internal controls are the responsibility of the entire organization. Therefore, in order to meet the goals and objectives of an organization, an effective internal control structure has to be owned and managed by all process owners.

Planning

In any well-managed project, the planning phase usually is the most important. Once support for implementation is garnered and the responsible team is identified, the next step is to develop the implementation plan. Several key areas should be considered in the plan, including a reasonable timeline, the number and types of resources needed, and the determination of roles and responsibilities of the implementation team. Because many competing priorities are being handled simultaneously throughout a healthcare organization at any point in time, the timeline should be flexible enough to accommodate shifting priorities. This might mean pushing the documentation of one process back and accelerating another, which requires flexibility from the implementation team and the full cooperation of management. Depending on the timeline urgency, the organization should consider the size of the implementation team and determine if the established team has sufficient knowledge of and experience with the covered processes. It is common for a team to be supplemented with additional resources from professional firms, which can help keep the timeline on target, document and test specific complex processes, or take advantage of lessons learned from other implementation efforts.

Scoping

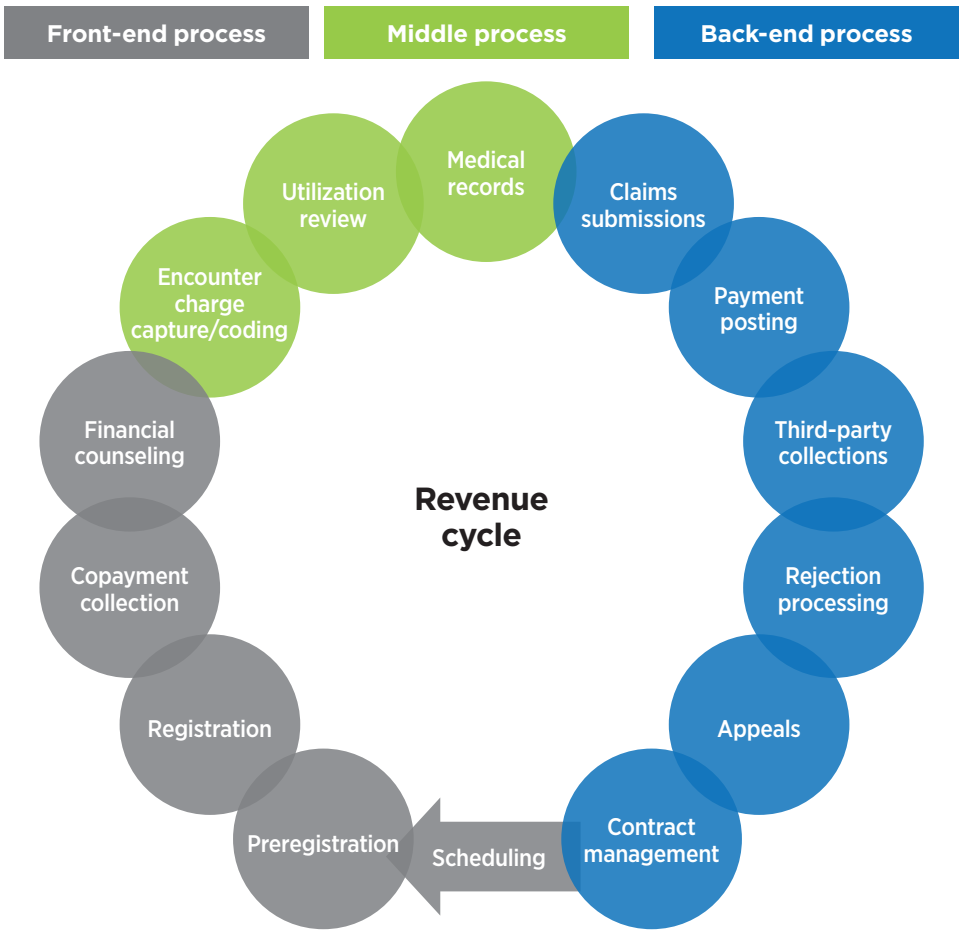
Scope is determined by the range of activities and by the period of record that are to be evaluated. Using COSO's guidance, an organization's management should focus on areas with the highest risks that could affect the organization's ability to achieve its strategies and objectives. Therefore, the scope should be considered before, during, and after the planning phase. When implementing the *2013 Framework*, the team should gain an understanding of the objectives and sub-objectives set by management (or governance) during the strategic planning process in order to identify the risks of failing to meet those objectives. Objectives can be categorized into three types (operations, reporting, compliance), and an objective can overlap categories. The team should evaluate the five components of the *2013 Framework* (control environment, risk assessment, control activities, information and communication, and monitoring activities) to determine how well an organization's internal control system is designed and operating to help management achieve those objectives (or allowing for timely communications if objectives will not be met).

There are several areas of risk healthcare organizations generally find significant, including but not limited to operational performance, quality of care, patient and employee safety, regulatory compliance, IT capacity and infrastructure, cybersecurity, and leadership capabilities and capacity. Those risks typically can be found in key processes such as revenue cycle; supply chain and vendor management; risk management; human resources; and financial statement reporting. Insufficient controls or the absence of proper controls in any of those processes can have considerable negative effects on the operational and financial aspects of an organization. Management should give strong consideration to the prioritization of significant risks in comparison with the availability of resources and the financial impact of the *2013 Framework* implementation. The first impulse might be to include all significant risk areas in scope, but once the key processes are identified, management should step back to consider the potential impact and likelihood of risk exposure and determine scope exclusions, if any.

For example, let's look at cybersecurity risk, which has increased dramatically over the past several years, especially with the widespread use of EHR in healthcare. It is a reality today for all organizations that the question is no longer *if* a breach will occur but *when*. Identifying key controls and control gaps is imperative to reducing the volatility in potential breaches. COSO has addressed this specific issue with January 2015 guidance by Mary E. Galligan and Kelly Rau with Deloitte. As the authors noted, "As businesses and technology have evolved, so has the *2013 Framework*. One of the foundational drivers behind the update and release of the *2013 Framework* was the need to address how organizations use and rely on evolving technology for internal control purposes. The *2013 Framework* has been enhanced in many ways and incorporates how organizations should manage IT innovation." As management evaluates the risks, especially the potential impact to the organization, consideration must be given to cyberrisk within all of the significant processes. This risk should be included in the scope of the *2013 Framework* implementation, but management should determine to what extent each process needs to focus on key controls that potentially mitigate such risk. As the authors further noted, "Which data, systems, and assets are of value at any particular point in time depends on the cyber attacker's motives. As long as cyber incidents continue to have a negative impact on the financial well-being of victim companies and continue to draw additional regulatory scrutiny, cyber breaches will continue to be high-profile events that draw a substantial amount of press."[4]

Another example would be the revenue cycle, which can be especially daunting (see Exhibit 4). It is one of the most important and most complex processes within a healthcare system, and it demands special attention. Given the risks and overall scope, breaking the revenue cycle process into components (such as front, middle, and back end) can increase its manageability. Management might not want to include all functional areas of the revenue cycle in scope but might drill down to the key processes within in order to manage the scope of the project at a reasonable yet effective size. Furthermore, keeping the organization's objectives in mind, the scope of revenue cycle should focus on the effectiveness and efficiency within the process, the proper reporting of patient revenue, and compliance with laws and regulations.

Exhibit 4. **Key revenue cycle processes Key revenue cycle processes**



Source: Crowe analysis

Meeting with external auditors

It is important to include the organization's external auditors in the planning for *2013 Framework* implementation. Generally, the external auditors have a comprehensive understanding of the organization's financial reporting structure and can provide further input about the scoping and focus of selected processes. Additionally, the external auditors may be in a position to rely on a portion of internal control monitoring conducted by the organization. Coordinating at this juncture can minimize possible redundancies in control-related evaluation; however, management should expect their external auditors to focus their interest and expertise on financial reporting objectives.

Communicating the plan

Throughout the planning process, open lines of communication with management should be maintained about project timelines, responsibilities, and scope. Once the relevant stakeholders are in agreement, the final plan should be presented to the appropriate governance body for discussion and approval. Maintaining communication and approvals at every step throughout the implementation process will increase transparency and ensure support of the implementation across the organization.

Phase 2: Assessment and documentation

Assess the existing control structure

Examining the existing control structure is an important step in the *2013 Framework* implementation. Similar to companies in other industries, the structure of healthcare organizations can vary greatly, often depending on size, location, and state, federal, legal, or religious requirements.

Centralized versus decentralized system structure

A significant part of an organization's control structure is its system structure. A centralized versus decentralized structure might dictate the implementation approach including the number of hospital system locations to visit, the departments and processes to consider, the number of personnel to interview, and the amount of existing control documentation to review. For example, if the organization's revenue cycle structure is centralized, management might find that the organization's business units share common business systems (e.g., EHRs) and processes including standardized internal control protocols and documentation such as front, middle, and back-end revenue cycle procedures. Alternatively, decentralized organizations often have a diverse array of business systems and processes that vary by business unit, resulting in nonstandard internal control processes and documentation. In addition to considering business systems and processes at the main corporate sites, management may need to have conversations with local and divisional process owners (possibly including visits to selected local and divisional business units) in order to better understand the control structure as a whole.

Some healthcare organizations may find it necessary to evaluate operations on a global level. In such circumstances, it is helpful to create a process map that documents control-related variability in order to prioritize travel and minimize disruption for staff members either traveling or serving as facility hosts for implementation team members.

Entity-level structure

Another important step is assessing the entity-level control structure. According to the Securities and Exchange Commission (SEC), entity-level controls are defined as controls "that have a pervasive effect on the entity's system of internal control such as controls related to the control environment."[5] The maturity of the entity-level control structure significantly affects the assessment and the associated results. For instance, does the organization currently have a formal ERM activity? If so, the organization already may have standardized processes for risk assessment, remediation design and implementation, monitoring, and reporting. Supporting processes such as ongoing management evaluations or separate evaluations driven by internal audit also may exist. Management can use these processes and the related documentation during the assessment. If the ERM activity is less formal, management may find that the responsibilities for risk assessment, remediation design and implementation, monitoring, and reporting are handled throughout the organization but also might not be performed at all. While the lack of a structured and coordinated approach to ERM does not in itself indicate a gap in the control structure, it may cause management to increase the number of locations visited or personnel interviewed in order to understand the control structure and associated specifics. In general, risk increases with organizational size and complexity; therefore, the need for a structured and coordinated approach to ERM – helpful in supporting an organization's efforts to drive strategy and achieve business objectives – increases.

Fraud risk assessment

Healthcare organizations are not immune to fraud schemes. Resource limitations, operational complexity, and constant change (both internal and external) provide a challenge to adopt adequate preventive controls that defer fraud and increase the likelihood of timely detection. The revised *2013 Framework* places additional emphasis on the need to consider the potential for fraud in assessing risks to the achievement of objectives (see Principle 8).[6] An understanding of the organization's risk for fraud will provide insight into where to focus management's assessment efforts and also potentially identify risks that could result in significant monetary or reputational loss to the organization if not properly mitigated. Although many organizations have informally contemplated fraud risks in the past, the *2013 Framework* highlights several points of focus that should be considered:

1. **Consider various types of fraud.** Fraud-related risk assessment considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.

2. **Assess incentives and pressures.** Fraud-related risk assessment considers incentives and pressures to commit fraud. Examples include management bonuses tied to the achievement of specific operational or financial measurements, which may inadvertently pressure management to artificially and fraudulently inflate numbers.

3. **Assess opportunities.** Fraud-related risk assessment considers opportunities for unauthorized acquisition, use, or disposal of assets; alteration of the entity's reporting records; or other inappropriate acts.

4. **Assess attitudes and rationalizations.** Fraud-related risk assessment considers how management and other personnel might engage in or justify inappropriate actions and considers situations and circumstances that may elevate the likelihood of inappropriate actions.

Fraud can occur in any process or functional area of a healthcare organization. Organizations have to be aware that potential fraud may transpire from within and from outside; therefore, risks to the whole system rather than just risks to internal processes need to be considered. Examples of potential fraud schemes include but are not limited to drug and supply diversions, billing patients for procedures and supplies that have not been performed or used, unauthorized access to patient information, alteration of financial reporting data, and vendor contract exploitation.
Fraud-related risk assessment leading practice involves discussing the potential for fraud with a pool of employees and possibly contractors at various levels and representing multiple geographies and functional areas. Asking open-ended questions about the potential for fraud often can provide management with information about what is actually happening in the field versus what management may expect or believe to be so. Even a small sample of interviews with the right individuals can provide meaningful data that informs possible mitigation strategies.

Multinational healthcare organizations – particularly those with business processes that involve or potentially involve government-employed healthcare professionals – also require multilayered approaches to fraud detection and control. These organizations often conduct specific risk assessment processes designed to identify potential risks and prioritize associated mitigation strategies. It can be helpful to share the results of these risk assessment discussions across internal teams such as internal audit, legal, compliance, and IT, at a minimum.

Furthermore, activities should include reviewing the most recent crime insurance application, reviewing prior theft incidents, and holding discussions with important operational, financial, legal, and compliance leaders at the national, divisional, and local levels to identify potential fraud scenarios and current controls. In addition, as part of an annual ERM risk assessment process, all senior leaders and governance members should be asked about their personal knowledge of any fraud risk assessment exposures that don't already have preventive or detective controls in place.

Documenting current processes and controls

As noted earlier in the "Planning" section, an implementation team should be selected and work closely with management throughout the process. After management has identified the processes that are relevant and significant to the control activities component of the *2013 Framework*, the next step is for the team to understand and document each process in order to detect internal controls (or control gaps) within those processes. Engaging leaders in each functional process and educating them on its purpose, benefits, and visibility to senior leadership and governance is vital to ensuring process owners' full participation.

1. **Identify the scope of a process selected for documentation.** Even after management selects key processes, it may not be possible or prudent to include every aspect of each process in a review of internal controls. This is especially true with large organizations that could have decentralized parts of a process that vary from the rest of the process. In these situations, management should evaluate the process against the entity's established risk tolerance to determine whether excluding the process and related controls is an acceptable risk to achieving the entity's objectives. For example, imagine the revenue process at a larger healthcare system. The system owns 10 hospitals but has determined that nine of the hospitals use the same billing system software while the other hospital uses different software. Management may decide to include the nine hospitals in the scope of the process documentation and exclude the other hospital. Because the other hospital uses a different billing system, there likely will be enough differences in the activities (both manual and system activities) for that hospital to require a separate process documentation if it were placed in scope. In this example, because one software system is being used for approximately 90 percent of the transactions and revenue (assuming equal-sized hospitals for this example), management may choose to focus resources on documenting the revenue cycle process of only the nine hospitals, assuming the selection sufficiently addresses the risk of achieving the determined objectives.
2. **Review existing documentation**. Provided that documentation is available, this step might give management and the team a good understanding of the current control structure and provide assistance to plan for location visits and personnel interviews. If the documentation is formalized and complete, it will allow the team to quickly confirm its understanding of business processes and focus on any process changes since the documentation was last updated. In our example, documentation might be provided to the team with a number of policies and procedures and some detailed employee manuals for performing various job responsibilities. The information can be a good starting point and allows the team to gain a more detailed understanding of some of the activities in the process. However, the documentation might be more tailored to explaining job responsibilities and specific job activities rather than explaining how a transaction flows through a system, where risks may exist for processing errors, and what internal controls are in place.
3. **Conduct interviews.** With the information obtained in its review of the existing documentation, the team can conduct personnel interviews. Interviews are a very important part of the process. The information gleaned during interviews provides the evidence to make informed decisions about the department's compliance with the process. It may be helpful to create an outline of interview questions or preliminary gaps identified to facilitate the interviews. If existing documentation is sparse or does not exist, an outline of interview questions that highlight the common control points in the processes being discussed would be beneficial. The geographic spread of some national and global organizations can make in-person interviews challenging and expensive; if necessary, interviews may be conducted using technology to eliminate the need for face-to-face meetings. In addition, using well-tailored questionnaires in such situations can also be very effective. In our example, given the complexity of a revenue cycle, the team may determine that it will take numerous interview sessions to fully understand the revenue process.

4. **Identify risks, controls, and gaps of existing processes.** During the review of existing documentation and while performing interviews, the team should begin to identify the risks, controls, and gaps related to the existing processes. For control structures that are mature and complete, this process might include noting changes since the last time that the process and control documentation was updated. For other control structures, building the foundation for control documentation and remediation plans might require taking detailed notes about process risks, controls, and related gaps.

5. **Prepare final process documentation with controls.** Whether an organization uses a governance, risk, and compliance system or manual tools such as word processing and spreadsheet software, the basic components of the documentation process are the same.

First, the team might want to contemplate developing current-state process narratives or flowcharts. In order to demonstrate sufficient understanding of the process, the following points could be considered for inclusion:

- Basic flow of transactions from initiation to completion
- Personnel involved in the process flow
- Controls performed as part of the process flow, as well as the personnel responsible for performing controls versus those responsible for reviewing control performance
- Systems used in the process and reports generated by these systems
- Segregation of duties, whether manual or automated

Given the various implementation approaches, one option for the team is to develop a risk and control matrix (see Exhibit 5). The control matrix is a document (generally maintained in a spreadsheet format or a specialized database application) that identifies all internal controls in the process in addition to specific descriptions and category attributes related to each control. Information captured for each control might include the following:

- Control number (assigned by management as a unique identifier)
- Control description
- Objective of control
- Risk associated with objective of control
- Frequency of control
- Control owner (role/title)
- Key or nonkey control type
- IT or manual control type
- Preventive or detective control type
- Fraud or non-fraud control type
- COSO principle (related to control)
- Financial statement assertion (related to control)

Exhibit 5. **Example of a risk and control matrix**

Control #	Process	Subprocess	Objective	Risk	Control	Frequency	Key/ nonkey	IT control	Manual/ automated
1.00	Revenue	Middle	To help ensure accurate and complete recording and billing of patient charges	Inaccurate or incomplete recording and billing of patient charges could result in patient dissatisfaction, potential regulatory noncompliance, and financial losses.	The EHR system will identify patient visits with a high risk of clinical documentation error and will route those visits to the clinical documentation improvement department at each hospital.	Continuous	Key	Yes	Automated
2.00	Revenue	Middle	To help ensure accurate and complete recording and billing of patient charges	Inaccurate or incomplete recording and billing of patient charges could result in patient dissatisfaction, potential regulatory noncompliance, and financial losses.	A clinical documentation improvement specialist will review the documenta-tion (e.g., EHR input screens, patient charts) for completeness, appropriateness, and accuracy of information.	As needed	Key	No	Manual
3.00	Revenue	Middle	To help ensure accurate and complete diagnostic or procedural coding	Inaccurate or incomplete diagnostic or procedural coding increases the risk of noncompliance with federal and state regulations and/or other health plan contract requirements.	Coders have restricted login access to the billing system.	Continuous	Key	Yes	Automated

Source: CHI

The last step is to validate the process and controls documentation with the control owners. It is important that the team obtains the control owners' confirmation of its documentation before performing the gap assessment or presenting assessment results to management. The goal of this step is to create accurate documentation; the team should avoid making an evaluation of quality or competency at this point, as doing so could inadvertently influence the completeness of the documentation obtained.

Another important point to consider is the management of the process and controls documentation. Updating the established process documents often is delegated to the relevant departments; therefore, many organizations keep process documents available on an internal shared drive with open access to department management.

Performing the gap assessment

The gap assessment occurs when management evaluates existing controls against the *2013 Framework*'s principles and points of focus to identify areas where the current design of internal controls is lacking to achieve an effective internal control system. In some cases, gaps identified will reveal design weaknesses in internal controls that could leave the organization vulnerable to serious financial reporting errors or misallocation of assets. In other cases, gaps identified may reveal merely areas of opportunities for improvement (e.g., cost-saving opportunities). There might even be situations where the level of control exceeds what is needed to mitigate the risk, allowing a reduction in controls and related cost while still adequately addressing the risks. A high degree of professional judgment can exist in determining what is and isn't a gap, which may require reviewing industry best practices or engaging professionals experienced in reviewing business processes for properly designed internal controls. The *2013 Framework* – its principles and points of focus – is a valuable guide to help determine where gaps may exist in the currently designed control structure of an organization or business process.

Take, for example, a potential gap in the clinical documentation improvement (CDI) area. Hospital systems may perform CDI reviews inconsistently before the medical bills are generated for transmission to payers. This gap is a design weakness in internal controls and could result in serious financial reporting errors through incorrect billing (versus services performed) or billing activities that insurance payers deny as having incomplete documentation. In addition, increased risk of overbilling at these hospitals could expose them to regulatory and legal issues. Another example of a gap might be the updates to the charge description master, given that the process might be decentralized and managed separately by local facilities. While this gap is not necessarily a design weakness that could lead to serious financial reporting errors (because the local facilities all have their own controls in place to restrict access), the decentralized nature of this design is deemed not as operationally efficient as if the organization had designed a process where these updates are managed by a single corporate management team (i.e., with cost-saving opportunities).

As the previous examples illustrate, gaps identified will have varying levels of significance to an organization. It often is valuable to classify gaps into categories of severity (e.g., high, moderate, low) or assign them locations on a heat map. This will help the organization identify which gaps are the most critical to focus on remediating and which gaps may not pose as serious a risk to the organization. Also, management might want to consider using other sources of information (e.g., revenue process and internal control guidance in the auditing profession, white papers) to help identify other types of internal control gaps in the process.

Illustrative tools

COSO has issued the *2013 Framework* and a companion document, "Illustrative Tools for Assessing Effectiveness of a System of Internal Control."[7] The COSO publication provides examples of various templates that are designed to help present a summary of results. It also provides guidance pertaining to form and use, and to organizational assessment and evaluation. Several practical examples are included on how templates can be used. As noted on page 2 of the COSO companion document under the "Templates" section, "The templates are not an integral part of the framework, and they may not address all matters that need to be considered when assessing a system of internal controls. Furthermore, they do not represent a preferred method of conducting and documenting an assessment. Their purpose is limited to illustrating one possible assessment process based on the requirements for effective internal control, as set forth in the framework."

The templates do not illustrate management's selection and deployment of controls to affect principles or its determination of scope, nature, timing, and extent of evaluating such controls embedded within the components. The facts and circumstances relevant to an assessment vary among different categories of objectives and among different entities and industries; therefore, the practical use of these tools also varies.

Phase 3: Remediation planning and implementation

Once the gap assessment has concluded and the deficiencies have been identified and rated, the organization can begin designing remediation plans and associated actions to implement the plans.

Remediation

Remediation plans should take into account the severity of each of the identified deficiencies by prioritizing the remediation of more severe deficiencies ahead of those deficiencies that are less severe.

Remediation plans generally include the following characteristics depending on the severity of the deficiency being remediated and the complexity of the remediation action:

- Indication of the related cycle, control number, and control description of the deficiency to be remediated (with the caveat that the control number and wording may not be available if no control currently exists)
- Description of the deficiency including affected IT system
- Notation of the responsible control owner or process owner
- Description of the remediation plan including, at a minimum, the remediation action to be performed, the person(s) responsible for the remediation action, and the estimated completion date for the remediation action
- Significant milestones or follow-up dates to monitor the remediation plan and its progress

Highly complex remediation plans may require elevated management attention to ensure successful implementation. Complex remediation plans may involve multiple processes and personnel, affect multiple IT systems, or require action by third-party service providers. For example, a deficiency in the coding process as part of the revenue cycle may require an adjustment of responsibilities among coding personnel as well as potential additional required documentation steps to be performed by the medical staff. These changes could involve the IT system administrators and potentially third-party service providers in order to remediate the noted deficiency.

Remediation implementation

Remediation plans may require significant time commitments from process owners or changes to current business processes. So, before beginning the remediation implementation process, it is important to confirm plans with and establish buy-in from those who will be involved. Successful and sustainable remediation efforts depend on input and commitment from process owners. Additionally, process owners will be able to assist in evaluating the effectiveness of the proposed remediation actions and also provide valuable insights into the remediation process including the reasonableness of objectives, proposed milestones, and the timing of project completion.
Once process owners provide input and confirm support, the remediation plans should be updated and verified. It is important to make sure the updated remediation plans remain focused on addressing the control deficiencies noted in the gap assessment phase and that the focus has not shifted to processes that were not identified as deficient or to processes with lower-rated deficiencies. A common challenge healthcare organizations face during the implementation phase is scope expansion. Ongoing attention is needed to ensure that control deficiencies are addressed as planned.

Phase 4: Design, testing, and reporting of controls

After the remediation plan and implementation phase (Phase 3), the next phase in the *2013 Framework* implementation is the test design, execution, and reporting phase (Phase 4), which includes selecting the controls to be tested, designing the tests of controls, executing the tests as designed, and then reporting on the associated results. It is preferable to wait on initiating Phase 4 until after the remediation plans in Phase 3 are tracked to completion so that the new controls created during the remediation work can be included in the initial testing of all selected controls. However, if the remediation plans are delayed or will take a long time to implement (e.g., more than three months), management should consider initiating testing of all other selected controls without waiting for the completion of the remediation work. While controls related to remediation eventually will need to be tested after those plans are completed, these controls generally would not be expected to be a large percentage of the total controls tested. Furthermore, any controls that were already existing (in other words, not related to remediation plans) will need to go through separate, additional remediation plans if they fail during testing, which is the strongest argument for not delaying their testing in order to wait for the completion of lengthy remediation plans from Phase 3.

Selecting controls for testing

After completing Phases 1, 2, and 3, the team and management might have identified numerous internal controls through the documentation of the entity-level controls, fraud risk assessment controls, and process controls for the selected, in-scope processes. Management also might want to assign a "key" or "nonkey" classification to each control to aid in the selection of which controls should be part of the *2013 Framework* implementation testing. This step ideally should be done when the control matrices are created. Key controls are the most critical controls for preventing the realization of risks and therefore are important in mitigating the risks of not achieving the organization's objectives. Nonkey controls generally are not as critical, as may be the case for duplicate controls or controls that have limited scope for select locations or specific transactions. The determination of key versus nonkey is at the discretion of management.

Design tests of controls

After selecting the key controls for testing (including new controls from remediation plans, if completed in a timely manner), the team is ready to design the individual procedures for testing each control. In designing a test of controls, it is important to understand both the risk to be mitigated and the related control description, which detail potential problems with the underlying activity or transaction that is intended to be mitigated. The control description details how the related control actually functions. Understanding both the risk to be mitigated and the control description allows the organization to design tests of controls that will apply to both the design and operating effectiveness of the controls rather than just operating effectiveness. For example, if a control functions as designed but does not fully address the risk being mitigated, then the tester may conclude that the control was not designed correctly, though it performed exactly as described. In this example, the tester would determine that the control has a design deficiency.

After understanding the risk to be mitigated and the related control description (which can be documented in the related control matrix), the organization should consider the nature, timing, and extent (scope) of testing in order to prepare test scripts, which are the detailed steps to be performed and include the nature, timing, and extent of testing along with the recommended documentation to be gathered. Different methods are used to perform tests of controls and to create test plans or scripts. Each method should be evaluated based on the complexity and timing of the underlying control. It is possible that multiple methods of testing may be needed – one type of test may not address every control.

The two common testing methods for controls related to *2013 Framework* implementation are observation and documentation examination. Examples of other testing methods include inquiry, re-performance, and data analytics.

- **Inquiry** – Inquiry involves asking control owners about a specific control and having them explain the control process. However, inquiry is not considered conclusive evidence on its own to determine the effectiveness of the control, and it should be combined with other testing procedures and evidence to garner a conclusion.

- **Observation** – During observation, the team watches the actual performance of the control. Observations work well when the team wants to observe a live, real-time application control such as a system generating a "not authorized" type of error message when an employee tries to access a part of an application in which the system is designed to restrict such access. In this case, the team would ask an employee to demonstrate an attempt to gain unauthorized access and observe the application denying the unauthorized access. The team also could obtain screenshots throughout the observation steps to have evidence of the test for the control testing work papers. Observation is also useful to validate the control design regarding manual procedures to understand whether the written process documentation is what is being performed.

- **Documentation examination** – Documentation examination requires understanding the entire population of transactions or activities that would necessitate the performance of a control. Examination may be performed to test for the proper design and operating effectiveness of the control. For example, a control may state that journal entries are reviewed and approved by appropriate personnel before entering into the system. Testing generally would include examining the supporting documentation generated by the performance of the control such as evidence that the journal entry was reviewed and that the amounts were included in the journal entry. The testing also would include the procedures necessary to verify that the IT system reports or other manually generated data used during the performance of the control were complete and accurate.

- **Re-performance** – Re-performance often is used for controls that may be manual and are performed on an infrequent basis. The team would re-perform the control steps in order to obtain the same testing results. Evidence obtained might include the original process documentation with notations on the results of procedures re-performed or a separate set of re-performance documentation with a comparison to the original control documentation.

- **Data analytics** – An organization also may use data analytic tools in order to test the design and operating effectiveness of controls. Data analytic tools are used to test information stored in an electronic format and usually include testing large populations of data using third-party software (e.g., computer assisted auditing techniques or spreadsheets). The tools can provide insights into populations and samples such as detailed population attributes and outliers that cannot be obtained solely by manual testing techniques.

- **Timing of testing** – The timing of control testing often is determined by the risk of control failure and the severity of the possible control deficiency. For example, the organization may want to test controls that have a higher risk of control failure (due to process complexity or turnover of key personnel, for instance) sooner than controls with a lower risk of failure in order to provide for a longer remediation period. Earlier testing, when appropriate, may decrease the duration of negative consequences (such as an increased likelihood of theft or fraud) resulting from the control deficiency.

- **Extent of testing** – The extent of testing depends on many factors including the importance of the process to the organization, the volume of transactions per period, the complexity of the control procedures, and the consequences of a control failure in dollars at risk or another relevant measurement such as reputational harm. Testing can be either statistically, nonstatistically, or judgmentally determined depending on the purpose of the testing and who may be relying on the results (e.g., external auditors). The organization should refer to the generally accepted auditing standards or the IIA standards for commonly accepted control testing criteria.

Perform test of controls and reporting

After designing the tests of the controls, the organization's next step might be to perform its control testing based on its testing plan and test scripts. As the tests are being performed, it is important to keep management updated concerning the progress of the testing and any issues or complications encountered. Management may be able to assist in finding solutions to issues and complications, which may help in meeting testing deadlines.

It is not uncommon for some controls to fail during initial testing in a *2013 Framework* implementation project. For any controls that fail testing, the team should work with the process and control owners to determine a remediation plan, including timing, to address the failure.

The results of control testing may be communicated to management either verbally or in a written format depending on the nature of the testing, the size and complexity of the organization, and the maturity of the internal control process. The format and content of the report may vary, but the following attributes generally are included:

- Description of the process and controls to be tested, including a description of the risks to be mitigated by the identified controls
- Listing of personnel involved in the testing, including control performers, process owners, and testers
- Description of tests performed, results, and determination of control deficiencies
- Rating of control deficiencies in order to assist in prioritizing remediation actions and plans
- Summary of management remediation plans, personnel responsible for remediation, and deadlines

Reports generally should be issued as soon as practicable after the completion of fieldwork. Many organizations agree to a time frame acceptable to all interested parties in order to ensure that testing results and remediation plans are communicated in a timely manner to those charged with governance in the organization. Additionally, plans for follow-up and retesting after the completion of remediation should be documented to promote accountability.
Every organization seeking to continuously improve its control structure and the related benefits is interested in optimizing the effectiveness of internal control.

Phase 5: Optimization of effectiveness of internal control

Alignment of risk and controls to the strategy and objectives of the organization

One of the primary ways to optimize the effectiveness of internal controls is to continuously align an organization's risk and controls to the organization's objectives. An organization adopts a mission and vision, sets strategies, establishes objectives it wants to achieve, and formulates plans for achieving them.[8] Over time, these strategies, objectives, and plans are updated and changed in response to new competitors, a changing regulatory environment, dynamic world economic conditions, internal resource limitations, and other challenges to the organization. Similarly, the alignment of risk and controls to the revised strategies, objectives, and plans also must be updated and changed.

COSO's objectives and components of internal control support the organization in its efforts to continuously align its risk and controls to its objectives. These objectives and components are relevant to an entire entity and to its subsidiaries, divisions, or any of its individual operating units, functions, or other subsets of the entity. An organization will discover that the *2013 Framework* will not only provide a basis for the initial alignment of its risk and controls to its mission and vision but will also provide an ongoing basis for realignment as the organization's strategies, objectives, and plans are updated and changed.

Process control structures

When an organization reviews its process control structures, it should consider various types of control activities such as reconciliation, supervisory, physical, and verification controls to determine the optimal balance or mix of controls that will mitigate the identified risks. Each of these types of controls can be designed as preventive or detective in nature. Controls also can be designed to be manual or automated.

Preventive versus detective controls

Control activities can be preventive or detective, and organizations usually select a mix that is optimal for their business model.[9] The major difference between preventive and detective control activities is the timing of when the control activity occurs. A preventive control is designed to avoid an unintended event or result at the time of initial occurrence (e.g., upon initially recording a financial transaction or upon initiating a patient billing process). A detective control is designed to discover an unintended event or result after the initial processing has occurred but before the ultimate objective has concluded (e.g., issuing financial reports or completing a patient billing process). In both cases, the critical part of the control activity is the action taken to correct or avoid an unintended event or result.

Manual versus automated controls

As with preventive and detective controls, most business processes have a mix of manual and automated controls, depending on the availability of technology in the organization.[10] Automated controls tend to be more reliable, subject to whether technology general controls are implemented and operating, because these controls are less susceptible to human judgment and error and typically are more efficient. However, the implementation of an automated control may not be practical due to limitations in the organization's current technology. In this case, a manual control could be designed to address the risk in question. It is important, however, to keep in mind the precision of the manual control when mitigating certain risks that might be complex or require specialized knowledge. Looking at the revenue cycle, an example of a manual control would be the documentation review (e.g., EHR input screens, patient charts) by a CDI specialist for completeness, appropriateness, and accuracy of information. The risk in this case would be the potential inaccurate or incomplete recording and billing of patient charges that could result in patient dissatisfaction, potential regulatory noncompliance, and financial losses.

Continuous monitoring

To assess the adequacy and effectiveness of internal controls, a continuous monitoring process may provide stronger support than scheduled monitoring that may occur on a periodic basis. Continuous monitoring usually involves the automated testing of all transactions and system activities within a given business process area versus testing based on sampling criteria, so continuous monitoring can offer a more comprehensive view of portions of the status of the control environment. The IIA Global Technology Audit Guide publication, "Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance," summarizes the following principles of continuous monitoring:

- "Purpose – consider the business objective and critical success factors.
- "Risk – determine likely obstacles that would inhibit the organization's success.
- "Response – align diverse sources of data to discover and corroborate emerging risks such as configurable conditions, changes, event logging, financial transactions, and unstructured data.
- "Timing – detect control issues in real time.
- "Action – track deficiencies for corrective action."[11]

Results of continuous monitoring should be made available to management as soon as practicable. Appropriate results also should be shared with corporate governance. An organization should consider the benefits of transitioning to a more continuous monitoring process as its risk mitigation capabilities and control structures mature.

Determining the root cause of control failures

The root causes of control failures often are elusive. Sometimes process owners and organizational personnel are reluctant to discuss the real reasons for a control failure due to fear of retribution or embarrassment. Other times, the real reason for a control failure is hidden behind the breakdown of two or more controls involving several processes, personnel, and perhaps even IT systems. In any case, it is important to determine the root causes of the primary drivers of control failures so that the remediation action can directly address the needed process enhancement.

Several formal methods exist to assist in determining the root cause of control breakdowns or other events. In its simplest form, root cause analysis is simply continuing to ask "why?" until the primary reason is identified. Each "why?" question is like peeling a layer of an onion away until only the core remains. It is only with the exposure of the core of the control failure that an organization can accurately create and implement remediation actions that directly address the root cause of the deficiency.

Conclusion

Healthcare organizations can apply the *2013 Framework* to strengthen the internal control structure, optimize the effectiveness of their control environments, and improve the efficiency of their governance, compliance, operations, management, and assurance functions, regardless of the size of the organization. The focus on strengthening key controls in an organization's existing control structure is vital in the rapidly changing landscape of the healthcare industry. Thus, it is recommended that every healthcare organization evaluate its risks and key controls to determine potential gaps that may require changes to policies and procedures, governance structure, and management oversight. With the implementation of the *2013 Framework*, an organization with effective controls will be able to:

- **Manage** the organization's ability to cope with rapid change
- **Provide** a strong foundation in order to accomplish significant goals and objectives
- **Improve** healthcare delivery

Key observations

1. The accomplishment of significant goals and objectives is affected by prioritizing and bringing attention to managing operational, financial, compliance, and IT processes.

2. Senior management and members of the board of directors – in particular members of the audit committee – generally should understand the *2013 Framework* and implementation benefits, costs, and approaches. Messaging and strong tone from the top will increase the likelihood of full cooperation through the in-scope departments.

3. Strong internal control functions can help mitigate many of the risks associated with current and future complex legislative, regulatory, and market pressures.

4. A successful implementation of the *2013 Framework* requires the commitment of management throughout the organization. Consideration should be given to the following steps for the applicable areas: planning and scoping; assessment and documentation; remediation design and implementation; testing of design, execution, and reporting; continuous monitoring; and optimization of effectiveness of internal controls.

5. Formally adopting the *2013 Framework* facilitates an increased understanding of the internal controls in existence, after which time improvements can be addressed in a prioritized fashion, resulting in reduced risk for all stakeholders.

Questions to consider

Management might want to consider the following questions when contemplating a 2013 implementation:

- What are the critical goals and objectives of our organization and the risks associated with them?
- How do we know we have effective internal controls in areas that are critical to accomplishing our goals and objectives (e.g., operations, regulatory compliance, reporting)?
- What type of commitment do we want to make when considering effective internal controls within key processes across the organization?
- Are the board and executive management supportive in strengthening the current internal control environment in order to successfully handle growth and complexity?
- What type of education is needed for board members, management team members, and process owners to understand the importance of internal control and the *2013 Framework*?
- What significant processes should be included in the scope, and what processes should be excluded?
- Do we have the expertise to implement the *2013 Framework*?
- Do we need any external consultants to guide the process and complete certain work and/or testing?

About the Authors

Annette Schandl, MSIB, CPA

Annette Schandl is a managing director at Crowe and has served in a dual role as a senior vice president in Denver, for Crowe since 2009. In this position, she oversees internal audit and consulting services for multiple Crowe clients, including CommonSpirit Health and Centura Health. Prior to joining Crowe, Schandl spent more than nine years with two Big Four firms focusing on financial attestation and global enterprise risk services. She had extensive experience in the healthcare field in various settings before transferring to public accounting. She has more than 20 years of wide-ranging healthcare knowledge focusing on hospital and physician practice operations, patient care, compliance, and financial business, including but not limited to orthopedic trauma, home health and infusion, anesthesiology, ophthalmology, and optometry.

Philip L. Foster, MBA, ARe, ARM, AIC, CPCU

Philip L. Foster, MBA, ARe, ARM, AIC, CPCU, is a senior vice president for CommonSpirit Health. Foster has 30 years of healthcare risk and insurance experience. He started his career as a hospital professional liability underwriter in New York City and then spent 10 years as a healthcare insurance broker and consultant specializing in alternative risk finance vehicles. More recently, Foster has spent 17 years within the enterprise risk management group of Catholic Health Initiatives (CHI), the past seven years as its chief risk officer. In this position, he has developed and implemented CHI's enterprise risk management program, which blends traditional internal control with leading-edge ERM activities. In this role, he works with CHI's senior leadership team and governance function on identifying, measuring, prioritizing, and monitoring critical enterprise risks as they relate to the organization's risk capacity and leadership's risk appetite. Foster also is the president and CEO of First Initiatives Insurance Ltd., CHI's wholly owned property and casualty insurance captive. He has extensive board experience, including on audit and compliance and quality and safety committees.

About COSO

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM), internal control, and fraud deterrence. COSO's supporting organizations are the Institute of Internal Auditors (IIA), the American Accounting Association (AAA), the American Institute of CPAs (AICPA), Financial Executives International (FEI), and the Institute of Management Accountants (IMA).

About Crowe: Building lasting value

Crowe LLP is a public accounting, consulting, and technology firm with offices around the world. Connecting deep industry and specialized knowledge with innovative technology, our dedicated professionals create value for our clients with integrity and objectivity. By listening to our clients, we learn about their businesses and the unique challenges they face. We forge each relationship with the intention of delivering exceptional client service while upholding our core values and strong professional standards. We invest in tomorrow because we know smart decisions build lasting value for our clients, people, and profession.

Learn more
Annette Schandl Managing Director +1.720.874.1770 annette.schandl@crowe.com

About CommonSpirit Health

CommonSpirit Health is a nonprofit, Catholic health system dedicated to advancing health for all people. It was created in February 2019 through the alignment of Catholic Health Initiatives and Dignity Health. CommonSpirit Health is committed to creating healthier communities, delivering exceptional patient care, and ensuring every person has access to quality health care. With its national office in Chicago and a team of approximately 150,000 employees and 25,000 physicians and advanced practice clinicians, CommonSpirit Health operates 142 hospitals and more than 700 care sites across 21 states. In FY 2018, Catholic Health Initiatives and Dignity Health had combined revenues of $29.2 billion and provided $4.2 billion in charity care, community benefit, and unreimbursed government programs. Learn more at commonspirit.org.

References

* As of the writing of this paper, for SOX Section 404 purposes, U.S. listed companies may use either the 1992 or 2013 version of "Internal Control – Integrated Framework." However, COSO has superseded the 1992 framework as of Dec. 15, 2014, and it is no longer available from COSO. The U.S. Securities and Exchange Commission has stated publicly that it may question the use of the 1992 version by U.S. listed companies as a suitable framework because it has been superseded by COSO.

1 "COSO Issues Updated 'Internal Control – Integrated Framework' and Related Illustrative Documents," COSO news release, May 14, 2013, coso.org/Documents/COSO-Framework-Release-05142013.pdf

2 "'Internal Control – Integrated Framework' – 20 Years Later," AICPA Insights, Jan. 18, 2012, blog.aicpa. org/2012/01/internal-control-integrated-framework-20-years-later.html#sthash.5rVBmeNg.prp8IRRB.dpbs

3 COSO, "Internal Control – Integrated Framework," Executive Summary, p. 3.

4 Mary E. Galligan and Kelly Rau, "COSO in the Cyber Age," January 2015, p. 1, coso.org/documents/ COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf

5 "Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934," SEC Interpretation, June 20, 2007, https://www.sec.gov/rules/interp/2007/33-8810.pdf

6 COSO, "Internal Control Over External Financial Reporting (ICEFR): A Compendium of Approaches and Examples," p. 70.

7 COSO, "Illustrative Tools for Assessing Effectiveness of a System of Internal Control," pp. 1-8.

8 "COSO – Internal Control – Integrated Framework, Framework and Appendices," p. 5.

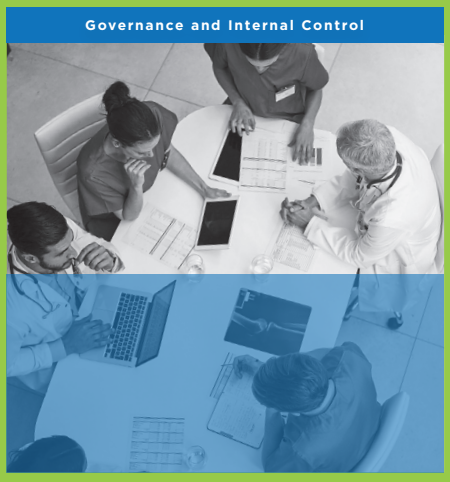
9 Ibid, p. 93.

10 Ibid, p. 94.

11 The Institute of Internal Auditors, Global Technology Audit Guide, "Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance," March 2015, 2nd edition, p. 6, na.theiia.org/ standards-guidance/recommended-guidance/practice-guides/Pages/GTAG3.aspx

Notes

Notes



COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org

Governance and Internal Control

COSO INTERNAL CONTROL – INTEGRATED FRAMEWORK:

An Implementation Guide for the Healthcare Provider Industry

COSO

Committee of Sponsoring Organizations of the Treadway Commission

coso.org