Are your internal controls in harmony with your business?

How the three lines of defense can work in concert to help your organization improve its performance

The better the question. The better the answer.
The better the world works.

EY
Building a better working world

Who is in control?

Contents

Introduction

Today, change is coming faster than ever, and there's more of it. Industries have been completely disrupted through digitalization and outsourcing. The sheer velocity of change has upended the business environment, and business models are constantly having to respond at an unprecedented pace. In fact, five years ago, we were talking about the fast pace of change, but that pace and the amount of change have only increased, with no slowdown in sight.

The pace of change has also affected organizations' internal controls. Risk events such as cybersecurity breaches, fraud and Foreign Corrupt Practices Act (FCPA) violations seem more frequent and more public than ever because the internet and social media require an organization to respond quickly to protect its reputation. We have seen regulatory activities increase over the last several years in response to the events in the marketplace. Additionally, there are internal control matters that, while not publicly discussed, may require significant time and investment to remediate.

So why then have many internal control programs not kept up with the times? Many companies have not materially modified the way they manage their system of internal controls since the inception of their internal control over financial reporting (ICFR) programs as part of their Sarbanes-Oxley Act (SOX) implementation. A review of an organization's internal control program may not only identify areas requiring control enhancements in response to changes in the business and regulatory environment, but also suggest ways to improve the efficiency of the ICFR program.

Organizations have an opportunity to clarify or reinforce the roles and responsibilities for their internal control environment, stressing that management has responsibility for internal controls. They may also be able to increase collaboration among the business, IT, internal audit (IA) and compliance functions; enhance communication with external auditors; and improve the effectiveness and efficiency of their internal controls.

Controls need to respond to the challenges of ever-changing business and regulatory landscapes.

Rapidly changing business landscape

Corporate failures in the early 2000s brought increased regulatory oversight and the need for companies to adopt a more compliance-focused mindset. During the financial crisis, the focus on survival was paramount: keep us out of trouble and streamline internal controls. For the next several years, leading performers focused on market reach, operational agility, cost competitiveness, stakeholder confidence, risk management and internal controls. And as the market was recovering, some companies made progress toward better alignment of risk management with changes in business models and emerging risks.

Despite all these efforts, many companies, as part of their compliance with SOX requirements, have continued to identify significant deficiencies and material weaknesses in internal controls.

COSO update

In 2013, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released an updated version of its Internal Control – Integrated Framework in response to the changes to companies' business models and increased expectations by regulators and other stakeholders regarding governance, risk management and fraud prevention.

COSO's enhancements in the 2013 framework were intended to:

- Address significant changes in the business environment and associated risks
- Specify criteria to use in the development and assessment of internal controls
- Increase the focus on operations, compliance and nonfinancial reporting objectives

While many companies worked to adopt the new framework, they may have missed an opportunity because, in some cases, it was treated as a mapping or documentation exercise instead of a way to refresh and optimize their internal controls.

How have changes to the business affected controls over time?

Regulatory response

As a result of the changes to the business environment over the last several years, regulatory activity has put more pressure on organizations to maintain strong internal controls. For example, in 2007, the Public Company Accounting Oversight Board (PCAOB) released Auditing Standard No. 5, "An Audit of Internal Control over Financial Reporting" (AS 5), which superseded Auditing Standard No. 2. It updated the requirements for performing and reporting on audits of internal control as required by SOX. Although the PCAOB's standards are directed at external auditors, companies are affected as the external auditors complete their internal control evaluations in accordance with the standards.

When AS 5 was adopted, the PCAOB announced its intention to monitor the implementation as part of its ongoing oversight activities. As a result of the findings noted during its inspections, the PCAOB released Staff Audit Practice Alert No. 11, "Considerations for Audits of Internal Control over Financial Reporting," to bring additional focus to the areas of concern.

Looking forward

In light of the PCAOB's inspection findings, organizations should consider the need to more fully implement the 2013 COSO framework. Additionally, regulatory developments continue on a global scale, e.g., the India Companies Act, creating an even greater need to take a holistic look at internal controls. Companies should determine whether their internal controls are keeping pace with changes in the regulatory environment in the countries where they operate. As the pace of change is expected to accelerate in the next several years, now is the time to rethink and enhance their internal controls. This is a good opportunity for organizations to think about their internal control program and ways to optimize their ICFR program. In short, this should be thought of as a value-added task, not simply a compliance exercise.

Does your organization have an effective and efficient integrated risk and control model?

Integrated risk and control model

Management owns the processes of identifying, managing and monitoring overall risks and internal controls, setting the tone at the top and fostering a risk-aware culture. Studies have shown that strong risk management and systems of internal control have a positive impact on long-term business performance and earnings potential.

Establishing a governance structure through the use of a well-defined and coordinated integrated risk and control model is the cornerstone of a strong risk management and ICFR program. Organizations must define clear ownership and accountability for risk management and internal control activities to enable effective coordination, communication and reporting.

When it comes to an integrated risk and control model, one size does not fit all. Many factors come into play, including industry, size, location, regulatory requirements, and risk culture. Even though each organization needs to design and implement an integrated risk and control model that aligns with its strategies and governance structure, some elements are common among all organizations.

In its 2013 position paper, The Institute of Internal Auditors (IIA) discussed the Three Lines of Defense (LOD) model. This model provides a simple and effective way to enhance communications on risk management and internal controls by clarifying roles and responsibilities.

One of the challenges facing organizations is implementing the right integrated risk and control model to address governance, as well as processes that enable management to gain comfort with the design and operating effectiveness of their internal controls.

Internal audit can play a key role by providing assurance around the program and either validating or performing the internal control testing. IA's independence, objectivity and internal control knowledge can allow management and the external auditors to place more reliance on its work. Clearly defined roles and responsibilities that are regularly updated regardless of organizational structure enable a more efficient and effective ICFR program.

Three Lines of Defense model

The three lines of defense need to be identified and deployed as part of the organization's overall risk and internal control strategy. However, no line of defense executes this strategy single-handedly; they must work together. In the context of an integrated LOD model, EY defines the three lines of defense as follows:

1 First line (operations and business units)

This group is composed of the line managers responsible for identifying and managing risks directly (design and operation of controls); they regard risk management as a crucial element of their everyday jobs.

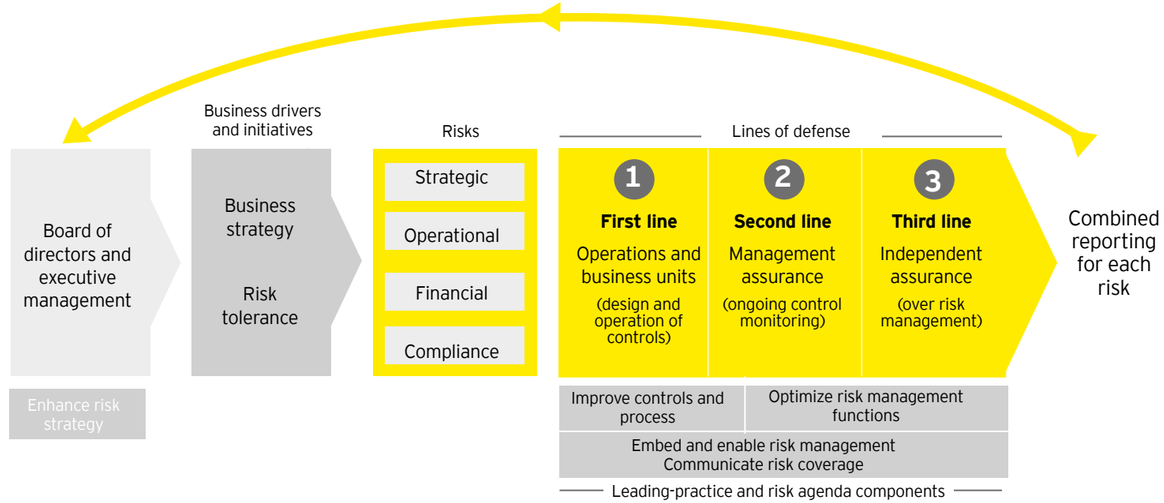
2 Second line (management assurance)

This group (typically including risk management, internal controls, legal, compliance, etc.) is responsible for the ongoing monitoring of the design and operation of controls implemented by the first line of defense, as well as advising on and facilitating risk management activities.

3 Third line (independent assurance)

The groups that are responsible for independent assurance over managing risks include internal audit, external audit and some regulators, as long as the scope and nature of their work align with the organization's risk management objectives.

Integrated risk and control model



Has your ICFR program kept pace with changes in the business and regulatory landscapes?

Even though we have been living with SOX requirements for over a decade, many companies have not matured or optimized their ICFR programs.

Only **34%** of respondents indicated the internal control program was mature*.

ICFR maturity assessment enabler

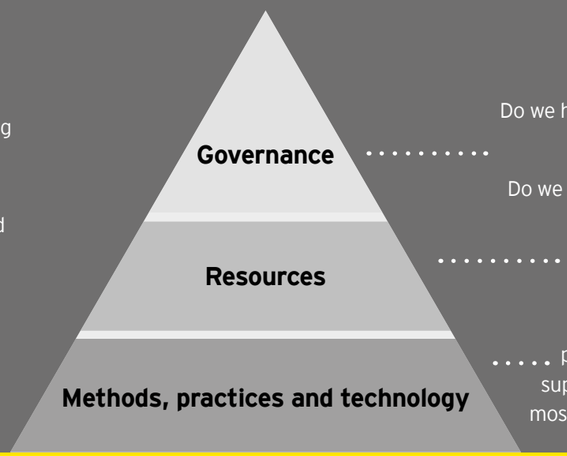
Leading organizations are using a model to assess the maturity of their internal control environments.

ICFR maturity assessment:

Evaluates current maturity of the internal control

Assists management in determining the future state

Provides implementation actions to reach the desired future risk and control environment maturity



Key areas:

Do we have the right oversight?

Do we have the right resources to deliver against our goals and objectives?

Do our methods, practices and technology support our business in the most effective way possible?

Sample of assessment factors:

Governance
- Internal control governance model
- Clear definition of the internal controls timeline

Resources
- Clear definition of roles and responsibilities
- Oversight of third-party providers
- Independent auditor reliance on management's control testing

Methods, practices and technology
- Control design and documentation
- Reporting of financial and non-financial control effectiveness
- Technology enablement

Maturity levels:

Level	Definition
1 Basic	Very minimal or basic level in relation to the individual component of the maturity model. There is a critical need for enhancements.
2 Evolving	The component exists in part but is inconsistently applied or not well-understood by management and relevant employees in a number of business areas. There is a significant need for enhancement.
3 Established	Activities are established, but there is a need for enhancement to become more effective and efficient.
4 Advanced	Activities are consistently applied and well-understood by management and relevant employees across the organization. There is limited need for enhancement to introduce leading practices in certain key areas.
5 Leading	Activities are established, consistently applied, integrated, regularly reviewed, aligned and coordinated across the organization. The practices are respected as leading practice and are viewed externally by other organizations as strong examples.

*EY ICFR Leading Practice survey

Key considerations to enhance your internal controls

At EY, we have helped organizations of different sizes and across sectors as they developed and implemented their initial ICFR programs and have continued to work with many of them as they have evolved their programs over time. We surveyed our internal audit professionals to gather information about ICFR leading practices and areas of improvement noted as they worked with our clients.

The survey encompassed 147 of our audit and advisory clients of varying sizes across the US, covering many industry sectors.

In light of the changing business environment, regulatory findings and our work with clients, we have seen a number of areas emerge as leading practices or opportunities for companies to enhance their internal controls.

Enhancement opportunities: **The topics below are the most common enhancement opportunities we see at our clients. These topics are discussed in the pages that follow, along with thoughts on the benefits of taking action.**

Governance

1. Governance structure
2. ICFR program
3. Changes to accounting standards
4. SOX Section 302 certifications

Control evaluation

5. Scope and mix of control testing
6. Management review controls
7. Information produced by the entity (IPE)
8. Population completeness
9. Control precision
10. Related parties
11. Deficiency impact analysis
12. Remediation of deficiencies

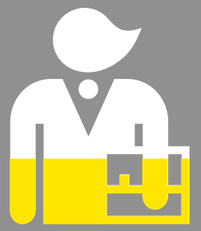
Technology

13. System implementations
14. Outsourced systems and business processes
15. Service Organization Controls (SOC) reports
16. Controls in the cloud
17. Segregation of duties
18. Cyber risk

Tools and techniques

19. Data analytics
20. Leveraging technology and tools

1 Does your governance structure maximize risk coverage and resources?



30%
of survey respondents indicated that internal control owner performance ratings are linked to the effectiveness of the controls for which they are responsible

57%
of survey respondents indicated that a formal internal control oversight committee was in place

Governance structure

As part of our survey, we asked questions about reporting lines and organizational structure in an effort to understand the current trends. We found that no one model emerged as the leading or most common.

The organization's management is responsible for establishing a governance structure that maps and assigns ownership and accountability for risk response activities across the organization. Whether your organization uses the LOD model or a model better suited to your organizational structure and culture, communicating the role of the various functions, including who has ownership of control testing, is critical.

At the end of the day, many people throughout the organization are needed to sustain a strong internal control environment, and it works better when all parties know their roles. For example, the resources responsible for maintaining ICFR documentation and those responsible for testing and monitoring control differ across organizations. There is no one clear answer, but what is clear is that companies need to have these roles defined so that things don't fall through the cracks.

While it might seem like an unimportant task after 10 years of complying with SOX requirements, many companies are taking a step back and documenting their ICFR program charter and rolling this out as part of their training programs. We see this as a leading practice.

Questions to consider

- Does your organization periodically reassess its internal control governance model?
- Does your organization perform a controls optimization exercise periodically?
- Is an assessment of risk coverage performed?
- Are current skill sets periodically reassessed to determine whether they are sufficient to address SOX requirements?
- Do you assess the amount of reliance the external auditors place on the company's work and whether modifications could enhance such reliance?

Benefits of taking action

- May drive better value with the business by aligning the risks that matter
- May reduce the cost of controls
- May result in increased reliance by the external auditors

Timing

- At least annually

2 Do you regularly update your ICFR program to respond to changes in the business and regulatory requirements?

87%
of survey respondents indicated that the ICFR program is aligned with COSO 2013.

27%
of survey respondents indicated that the internal control function was very mature or leading-practice.

ICFR program

In 2004, many companies were issuing their first reports on ICFR. However, controls that were appropriate at the time of implementation may no longer be effective given the fast pace of change on the global stage. Since then, shifts in the regulatory environment have affected companies broadly, and business models have changed significantly with technology breakthroughs that have, in some instances, disrupted the marketplace.

Leading-practice organizations have established a sustainable process to periodically refresh their ICFR program to respond to changes in the marketplace. For example, COSO's 2013 framework includes enhancements intended to (1) address significant changes in the business environment and associated risks; (2) specify criteria to use in the development and assessment of internal controls; and (3) increase the focus on operations, compliance and nonfinancial reporting objectives. This is just one example of how our clients have done a more in-depth refresh of their ICFR program and used it as a platform to make more holistic changes and improvements.

Questions to consider

- Have you aligned your internal control framework with COSO 2013?
- Do you have a process to identify significant changes in the business and regulatory environment and assess resulting risks to the organization?
- Do you periodically refresh the criteria used to develop and assess controls?
- Have you increased the focus on operations, compliance and nonfinancial reporting objectives?

Benefits of taking action

- Clarifies roles and responsibilities across the three lines of defense
- Can be used to align internal control definitions and risk assessment criteria
- Encourages involvement by the C-suite
- Enables alignment with the organization's strategic objectives

Timing

- At least annually and monitored for changes on a regular basis

3 Are changes to accounting standards identified and implications to the business addressed on a timely basis?

Changes to accounting standards

As the rate of change within the business and regulatory landscapes continues to accelerate, staying on top of accounting changes and how they apply to an organization's business model will remain an ongoing challenge. Many companies typically assign responsibility for technical accounting interpretation to their external reporting function. Responsible parties then typically subscribe to mailing list(s) and monitor website updates from the Financial Accounting Standards Board (FASB), International Accounting Standards Board (IASB) and Securities and Exchange Commission (SEC), in addition to working with their external auditors. Given the frequency of "updates," the increasing complexity and changes to organizational business models, the risk exists that standards may be misinterpreted and disclosure requirements within quarterly reporting may be missed. Accounting change is more than accounting and more than change. Companies that handle the transitions well will find themselves in a position of improved performance from IT to processes and related governance and controls.

Questions to consider

- Do you know where to obtain assistance with interpretation when needed?
- Are internal controls evaluated to confirm that they are adequately designed to address these changes?
- How are changes to accounting standards communicated to those responsible for the related internal controls?
- Have you evaluated the impact of accounting change not only on the actual accounting but also on governance, people, process, technology and related internal controls?

Benefits of taking action

- Enables compliance with regulatory requirements
- Facilitates appropriate up-front interpretation and application of accounting standards to your business
- Enables open lines of communication across the organization

Timing

- Ongoing to respond to changes on a timely basis

A well-documented and well-understood ongoing process is critical to staying abreast of accounting standards changes.

4 Is your SOX Section 302 certification process conducted with the appropriate level of diligence?

While many companies may feel they have a good SOX Section 302 certification process, some may have become complacent, going as far as rubber-stamping certifications, introducing even more risk to their organization.

SOX Section 302 certifications

From what we have seen over the last several years, implementing the right processes to enable executive leadership to gain comfort with the design and operating effectiveness of their internal controls is one of the challenges facing organizations as they address compliance requirements.

You can take these steps to enhance your SOX Section 302 certification process:

- Select a SOX Section 302 certification program leader responsible for reviewing the listing of 302 participants and reviewers, distributing the quarterly questionnaires, gathering responses from the functional leaders and communicating the results to the CEO and CFO
- Identify functional leaders that will collect and review their area's questionnaires and act as independent reviewers, challenging the status quo and pushing the CEO and CFO to make certain they are comfortable with the responses
- Create a questionnaire that certifiers will need to complete; the type of questions each certifier receives may depend on a number of factors, including the certifier's role in the organization and the business unit to which the 302 certifier belongs
- Send any questionnaires with noted issues to the functional leaders immediately
- Select a tool that will be used to administer the questionnaire and approval/certification process
- Confirm that control objects are processed and documented appropriately through the use of your company's calendar functions for reminders, escalations and notifications

Questions to consider

- Has your organization named someone as the SOX Section 302 program leader?
- Does your organization use questionnaires and set reminders to facilitate the process?
- Has your organization implemented a tool to administer the program?
- Has your organization identified the functional leaders, and do they understand what is expected of them?
- Have you considered streamlining the SOX Section 302 process by embedding it into the disclosure committee process?

Benefits of taking action

- Enables compliance with regulatory requirements
- Provides more visibility into and oversight of the organization's internal control environment
- Enables identification of issues throughout the year rather than at year-end
- Provides more comprehensive information for the presentation of quarterly findings

Timing

- Quarterly and as needed as control environments change

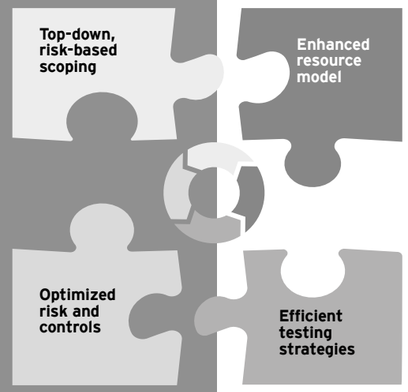
5 How do you select and monitor the right scope and mix of controls?

Scope and mix of controls testing

Many would agree that a top-down, risk-based model with a focus on financial statement assertions and disclosures is the appropriate methodology; however, we are still seeing challenges with scoping. It is also no surprise that the mix of controls is a lever that can be pulled to help create efficiencies. Controls optimization – e.g., coordination of activities across various functions, the use of automation and centralization of controls, and the periodic update of the controls mix in response to changes in the business – is not a new concept. In fact, we have been talking about it for years. But controls optimization should not be a onetime exercise – it should be done periodically to keep pace with changes in the business and regulatory environments.

What is the right scope?
- Use a top-down, risk-based model
- Focus on financial statement assertions and disclosures
- Understand the implications of changes in the business

What is the right mix of controls?
- Optimize controls, e.g., automation and centralization, and prevent vs. detect groupwide controls
- Leverage monitoring controls where appropriate
- Update controls mix for changes in business and systems



Who should monitor?
- Use remote, offshore or outsourced resources as appropriate
- Consider using variable or seasonal resources
- Select resources that are objective and have the necessary skills and competence

How do you monitor?
- Use risk-based control testing
- Establish a variable testing model
- Establish an approach for rollforward and remediation testing
- Define a deficiency identification and aggregation process

Questions to consider
- Have you performed an internal controls optimization exercise evaluating the mix of controls?
- Have you evaluated your internal audit and internal control function risk coverage for optimization opportunities?
- Have you considered alternative monitoring capabilities, e.g., offshore, by third parties or by different parties in-house?
- Have you evaluated the relevant IPE and IT general controls in your ICFR program?
- Have the control owners received training on the importance of IPE and IT general controls?

Benefits of taking action
- May improve overall efficiencies in the execution of the ICFR program
- May reduce the cost of controls through the use of automation
- May reduce the risk of financial reporting misstatements or restatements
- May improve awareness and accountability among control owners

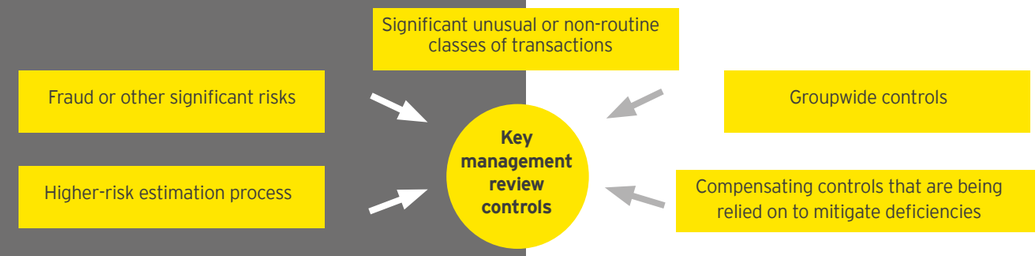
Timing
- When controls are executed
- At least annually – control owner training

6 Are management review controls designed and executed appropriately?

Management review controls

Management review controls are detect and correct controls that are performed by individuals, generally in management positions, with the appropriate competence and authority, who, as part of their job responsibilities, review financial statements, account balances, account analyses, estimates, reconciliations or other data. For example:
- Internal controls designed to determine that important estimates are complete and accurate and that potential errors are detected and corrected, e.g., goodwill impairment, business combinations and income taxes
- Internal controls designed to determine that other internal controls continue to function as designed, including review of account reconciliations
- Direct entity-level controls designed to identify unusual trends or inaccuracies in financial reporting, e.g., quarterly balance sheet fluctuation analyses

Typical areas of management review controls



Questions to consider
- Does management understand the purpose of the review and the risk it is intended to address?
- Do control owners understand the required documentation to support execution of the controls?
- Does management receive periodic information updates and training on management review control requirements?
- Have you evaluated the thresholds you are using and obtained alignment with all stakeholders?

Benefits of taking action
- Enables the organization to effectively address business risk
- May reduce the risk of financial reporting misstatements or restatements
- Enhances awareness and accountability among control owners

Timing
- Ongoing to respond to changes on a timely basis
- At least annually – management training

7 Are you considering the completeness and accuracy of IPE in your controls?

IPE

IPE is any information provided by the entity using the entity's IT applications, end-user computing tools or other means. It is used by management, be it in electronic or printed form, in the performance of controls. Ineffective controls over system-generated data or reports continue to be a common finding related to ICFR.

Every review control that relies on end-user computing should be accompanied by evidence of IPE completeness and accuracy to give management confidence that data used to make critical decisions is appropriate.

Questions to consider

- Are the risks related to IPE properly addressed?
- Have you evaluated the relevant IPE and IT general controls in your ICFR program?
- Have the control owners received training on the importance of IPE and IT general controls, and are they aware that controls need to be executed with complete and accurate information?

Benefits of taking action

- May improve awareness and accountability among control owners
- May enable reliance by the external auditors
- May reduce the risk of financial reporting mis-statements or restatements

Timing

- When controls are executed
- Ongoing
- At least annually – control owner training

When companies internally gather evidence of the design and operating effectiveness of controls, they should consider and document the completeness and accuracy of the evidence.

Use the **5 W's + How** to document evidence

Where does data come from?

Who performs the review?

When is data received?

What procedures does the process owner perform for reliance of IPE?

Why is the IPE utilized in the control?

How is data compiled or generated from the system?

8 When is population completeness important?

Population completeness

You may find that data previously provided as population evidence to the auditors is now being questioned with respect to completeness. It is important that no data is inadvertently omitted or excluded, thus misrepresenting the population. One way to reduce the burden of gathering and retaining the evidence of completeness for reports is to benchmark the report program and secure its access so that users cannot modify it or exclude content once it is extracted from the system. If the reports are controlled this way and IT general controls are effective for the system that produced the reports, the evidence of completeness may be needed only once during the year.

Reports used as population in the testing of IT and business process controls should be accompanied by evidence that the reported data completely reflects the information contained in the system and that it was not inappropriately limited or modified when the reports were generated.

Questions to consider

- Have you confirmed your understanding of documentation requirements for population completeness with your external auditor?
- Have you considered automating your completeness evidence?

Benefits of taking action

- Enables timely communication of requirements to control owners to establish awareness and enhance compliance
- Demonstrates proactive stand on controls and collaboration

Timing

- At the beginning of the audit cycle
- During status meetings with the external auditors
- During control redesign efforts
- During system upgrades

9 Are your controls precise enough to detect significant issues?

The overall goal of management estimate testing is to validate that the issuer's assumptions and estimates underlying the valuation of assets and liabilities are reasonable.

Control precision

Management estimates, including their precision, have become a growing area of focus due to their subjectivity and, in some cases, financial significance. Common findings include the absence of controls testing over the development of an estimate and the absence of evaluation of the reasonableness of the assumptions underlying the estimate.

Similar to management review controls, the following items should be top of mind when assessing management's controls regarding key estimates:

- Determine the method, significant assumptions and completeness and accuracy of information used
- Gather and evaluate information, including available contrary information, and apply it in determining the amounts to be recorded or disclosed
- Evaluate which key assumptions drive the estimate
- Analyze whether management's review of those assumptions is reasonable given the support for the estimates

Questions to consider

- Does management have an understanding of the requirements for its review of internal controls — e.g., is there annual refresh training on control owner requirements?
- Are controls evaluated periodically to confirm that they are designed to address emerging areas of focus?
- Is control precision evaluated for areas of significant estimation, including fair value measurements, impairments, reserves and income taxes?

Benefits of taking action

- Can have a positive effect on business performance
- May result in a reduction of financial reporting misstatements or restatements
- Provides better awareness and accountability among the control owners

Timing

- Ongoing to respond to changes on a timely basis
- At least annually — management training

10 Do you know who your related parties are?

Companies should revisit the controls they have in place to identify, account for and disclose transactions with related parties and executives, and significant unusual transactions.

Related parties

When thinking about PCAOB Auditing Standard No. 18 (AS 18), related-party transactions come to mind; however, the standard goes beyond these transactions and includes:

- Relationships and transactions with related parties
- Significant unusual transactions
- Financial relationships and transactions with executive officers

The PCAOB developed the standard to focus the auditor's attention on areas that have been associated with risks of fraudulent financial reporting and error. To address these risks, companies should also focus on these transactions.

Questions to consider

- Does your organization have a confirmation process that includes key stakeholders to evaluate existing and new relationships?
- How do you obtain completeness in reporting of related parties and their transactions in a timely manner?

Benefits of taking action

- May expedite the disclosure process
- May reduce audit fatigue
- Enhances risk management activities

Timing

- Quarterly confirmation process

Companies should maintain the following documentation:

- The names of the company's related parties and the business purpose for entering into the transaction
- Background information on the related parties (for example, physical location, industry, size and extent of operations)
- The nature of any relationships, including ownership structure, between the company and its related parties
- The transactions entered into, modified or terminated, with its related parties and the terms and business purposes of such transactions

11 Does your organization conduct an impact analysis once a deficiency is identified?

When deficiencies related to business processes or key financial systems and controls are identified, performing additional procedures to determine whether anything "bad" happened is the next step.

Deficiency impact analysis

When deficiencies are identified during the fiscal year and internal controls are deemed ineffective, compliance teams can help management implement action plans that reduce the risk to the organization and may prevent the need for expanded external audit procedures. For example, if there were segregation of duties (SOD) conflict violation deficiencies — such that programmers had access to production — performing an impact analysis could confirm that no unauthorized changes were made. This analysis should include obtaining a complete population of changes made to the system where the SOD violation occurred and reviewing them to confirm that all were approved, tested and appropriate. This step clearly goes beyond simple remediation. Removing programmer access to production addresses the SOD violation and prevents the deficiency from continuing, but it does not address the risk that inappropriate access was exploited when the deficiency existed. A targeted impact analysis confirms that the business process or system can be relied upon to process financial transactions accurately despite the SOD deficiency.

Questions to consider

- Does your organization consistently perform a risk and impact assessment when deficiencies are identified?
- Does your organization review evidence, logs and changes to confirm that deficiencies were not exploited?

Benefits of taking action

- Obtains evidence that the deficiencies were not exploited
- Provides evidence to potentially prevent additional audit procedures or reduce audit follow-ups
- Minimizes the effect of control deficiencies

Timing

- Immediately after the deficiencies are identified
- Prior to finalizing management's SOX Section 404 conclusions

12 Can delaying remediation of deficiencies today turn into significant deficiencies in the future?

Management should define and implement specific remediation plans for all deficiencies. If the plans are in place but span multiple years, temporary compensating controls may need to be implemented to mitigate risks.

Remediation of deficiencies

Management may not be aware of the consequences of postponing remediation of identified deficiencies or may have no plans to remediate the deficiencies. Some deficiencies are more challenging or may take longer to remediate due to people or process complexity or due to system limitations. For example, management might decide to replace an entire system rather than fix a multitude of issues. Sometimes, the system replacement is a part of the IT architecture road map — a consequence of the company's growth and movement to newer computing platforms. These circumstances may lead to multiple system and business process deficiencies that are not remediated for a prolonged period.

Whether deficiencies repeated over multiple audit years will trigger a significant deficiency or material weakness conclusion in any given fiscal year is a management and external auditor decision, and every circumstance differs depending on whether management plans to address the issues within a reasonable time frame. However, the company should have sufficient compensating controls in place while the issue exists.

Questions to consider

- When individual deficiencies are evaluated in the aggregate, could this lead to a significant deficiency or material weakness conclusion?
- Does your organization have a process to formally revisit prior year deficiencies to determine whether they have been remediated or adequate action plans are in place?

Benefits of taking action

- May mitigate the risk of financial reporting misstatements
- Demonstrates a proactive approach to internal controls
- Avoids the need to carry over deficiencies by determining and addressing the root cause of the deficiency

Timing

- As part of the quarterly certification process
- At least annually
- Prior to finalizing management's SOX Section 404 conclusion

13 How do system implementations affect the internal control environment?

System implementations

When IT applications used to process transactions that are reflected in financial statements undergo major changes, compliance teams and internal auditors have a unique opportunity to help management achieve a successful implementation. These changes may involve technology-enabled business transformations, IT service provider changes, system upgrades, infrastructure migrations and anything falling into the category of "move to the cloud."

IT application implementations often introduce new control capabilities that allow the organization to better leverage its significant IT investment and reduce risk by taking greater advantage of automated controls within the business processes. However, IT application implementations also introduce new risks, such as increased risk of failure to make the necessary customizations to the system, correct known pre-implementation errors, completely and accurately convert or transfer data or appropriately restrict access to sensitive transactions, affecting the IT application's ability to support effective internal control that enables accurate financial reporting.

The design and implementation of internal controls are key to a successful system implementation.

Questions to consider

- Has management embedded control considerations into their system development process for financially significant IT applications?
- Do business and IT representatives actively participate in defining relevant risk and control considerations?

Benefits of taking action

- Reduces the risk of financial transaction misstatements due to erroneous system functionality
- Reduces the risk of inappropriate changes to key systems
- Avoids system outages and operational problems after go-live
- Promotes understanding within the business as to how system changes could optimize the control environment
- Drives communication and further links IT and business process together within the organization

Timing

- The planning phase of system implementations
- Planning and testing prior to go-live to help reduce post-implementation issues

14 Where does responsibility and oversight for outsourced systems and business processes reside in your organization?

Outsourced systems and business processes

Outsourcing systems and business processes does not absolve user entities of their responsibility for an effective internal control environment.

Report type	SOC 1	SOC 2
Communication purpose	Opinion on controls at a service organization relevant to user entities' control over financial reporting	Opinion on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy
Intended audience	User entity and an auditor of its financial statements	Management of service organization, user entities and other specified knowledgeable parties

Third-party service organizations operating information systems and providing business process services supporting financial reporting have grown increasingly interconnected with their customers (user entities). This can lead to an assumption that the service organization is solely responsible for having an effective internal control environment on behalf of management. However, management is responsible for assessing the effect of the services provided by the service organization on ICFR, including the risks of material misstatement. As a result, user entities are requiring more information and assurance about internal controls from third-party service organizations. To respond to this demand, a third-party service organization may provide a Service Organization Controls (SOC) report to its user entities.

Management is responsible for assessing the SOC report to determine that it covers the relevant scope (the system including the IT applications, policies and procedures, and service organization locations) and time period, and contains a sufficient and appropriate level of communication concerning the design, implementation and operating effectiveness of controls to address the risks of material misstatement. Compliance teams and internal auditors may assist with assessing the SOC report, as well as controls implemented by management to address the complementary user entity controls (CUEC) identified by the third-party service organization as necessary to achieve certain control objectives or criteria included in the SOC report. Compliance teams and internal auditors can also assist management with an assessment of the impact of deviations in the design, implementation or operating effectiveness of controls at the service organization identified in the SOC report.

Additionally, the service organization may outsource certain services to a subservice organization and carve out those services from its SOC report. A subservice organization may not provide a SOC report to user entities; however, controls at the subservice organization may be relevant to the user entity's internal control environment. Compliance teams and internal auditors have an opportunity to assist management with assessing and minimizing risks inherent in outsourcing systems and business processes while managing costs of effective internal control.

Questions to consider

- Have formal roles and responsibilities been established for all outsourced processes?
- What specific services, including control objectives, controls and applications, are being provided by third parties?
- Are expected controls included in SOC reports and tested properly and for a sufficient period of time?
- Do you proactively address CUECs through existing controls to reduce overall ICFR costs?

Benefits of taking action

- Proactively monitors performance of system service providers
- Avoids surprises regarding CUECs
- May prevent late identification of deficiencies

Timing

- During the planning and contracting phases
- Controls should be in operation for the fiscal period

15 What can you do if a SOC report is not available?

Understanding the availability and content of the SOC reports prevents the expense of additional audit procedures.

SOC reports

Occasionally, a company may have a third-party service organization that operates information systems and provides business process services supporting financial reporting yet does not have a SOC report available. Or the report does not cover the relevant scope (the system including IT applications, policies and procedures and service organization locations) or time period. There are two types of SOC reports. A Type I report provides an opinion on an examination of a description of a service organization's system and the suitability of the design of controls to achieve the stated control objectives as of a certain date. A Type II report provides an examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls to achieve the stated control objectives over a period of time, typically 6 to 12 months. If an appropriate SOC report is not available, management, with the assistance from compliance teams and internal auditors, should determine whether relevant controls exist at the user entity (and are included in the entity's ICFR assessment) over the services provided by the service organization to mitigate the risks of material misstatement that may arise from the transactions processed and services provided by the service organization. If sufficient controls do not exist at the user entity, management, with assistance from compliance teams and internal auditors, may need to perform tests of controls or substantive procedures at the service organization. Management may also elect to arrange for an independent auditor to perform tests of controls or substantive procedures at the service organization, if necessary.

Questions to consider

- Does your organization consider the vendor's ability to provide SOC reports when evaluating potential vendors?
- Do you evaluate the control environment at third-party providers before entering into a contract, especially for processes that support strategic business capabilities?
- Is the "right to audit" clause inserted in your organization's key contracts?

Benefits of taking action

- May avoid deficiencies
- Increases transparency of control execution by third-parties
- May reduce audit costs
- Enables better service provider accountability

Timing

- During the planning and contracting phases
- During periodic communications with procurement
- As part of designing your vendor management oversight function

16 When systems move into the cloud, can you expect controls to follow?

Buyer beware: when entire systems or their components are moved into vendor-managed solutions, due diligence related to controls will pay off big.

Controls in the cloud

Cloud computing is more than a buzz phrase; it has become a force in the marketplace. In fact, moving "into the cloud" has become common as companies seek to reduce costs, streamline operations and refocus their resources on core competencies. As cloud providers proliferate, many smaller IT service providers offer minimal or no independent assessment of their services and may not have an appropriate internal control environment or security infrastructure to protect your critical business data.

The cloud is evolving rapidly, giving companies a variety of choices. But like most technology changes, the cloud presents its share of risks and challenges that are often overlooked or not fully understood. For example:

- **Infrastructure and architectural risks.** These hard return risks arise if providers do not achieve performance requirements that organizations and the providers agree to and define in the service-level agreements at the outset of the contract.
- **Standards and interoperability risks.** It is vital that the organization's systems and those of the provider can communicate with one another.
- **Regulatory and compliance risks.** Organizations using cloud computing services, and particularly software-as-a-service (SaaS), have lower transparency into security controls and processes that providers implement.
- **Cloud vendor management and governance.** Contractual risks stem primarily from the types of contracts that clients enter into with cloud service providers (CSPs).
- **Business continuity risks.** Cloud users are depending on their CSPs' business continuity program and disaster recovery capabilities.

Questions to consider

- Did the organization consider a service provider's maturity before entering into a contract?
- Has a "right to audit" clause been included in the contract?
- Has your organization asked for a SOC2 Type II report if it is an ICFR-relevant system?
- Has IT management been advised about the alternatives for mitigating risks if no report is available or the service organization does not plan to provide one?

Benefits of taking action

- Promotes an effective control environment
- May prevent operational difficulties
- May prevent deficiencies

Timing

- Discuss the need for controls with procurement in the planning stages of the sourcing project
- Review available vendor documentation and request SOC reports during the request for proposal (RFP) process
- Verify that controls are in operation throughout the fiscal period

17 Why is segregation of duties a ticking time bomb?

Without an automated GRC tool, major enterprise resource planning systems may not have adequate controls over SOD conflicts.

31%
of respondents used an automated solution to evaluate SOD as it relates to user access.

Segregation of duties

In today's complex system landscape, segregation of duties (SOD) conflicts may exist in a company's key financial processes for many years without any negative effect or detection. However, when issues arise, they may have consequences for financial statement reporting. For example, a disgruntled employee with excessive access rights may "inadvertently" delete all of the inventory records for the year. Fraudulent transactions may be posted without being detected. Employees may circumvent spending or purchasing limits through a combination of roles. The existence of numerous SOD conflicts often comes to light when a company decides to implement a governance, risk and compliance (GRC) tool. Given the large number of financial system users and various ways of configuring and granting access rights, the initial runs of automated procedures to detect SOD conflicts may result in identification of thousands or tens of thousands of conflicts, some of which are false positives.

Compliance functions can help the company to address SOD risks proactively if they partner effectively with different functions within the company. While there are risks of SOD conflicts within IT processes that must be mitigated through appropriate controls, the majority of a company's SOD controls must reside within business processes to effectively mitigate the risk of fraud or errors. To avoid significant SOD deficiencies, even in the absence of an automated tool, steps can be taken to minimize risks. The key is a proactive approach that analyzes the risks and implements appropriate controls.

Questions to consider

Does your organization:

- Have a process-specific SOD rule set based on the risk of misstatement?
- Have a process for handling exceptions?
- Have controls to enforce the rules?
- Gather evidence of an annual rule review and approval?
- Gather evidence of the assessment of SOD violations to show that deficiencies were not exploited?
- Adjust the control framework to align compensating controls if SOD conflicts cannot be avoided?

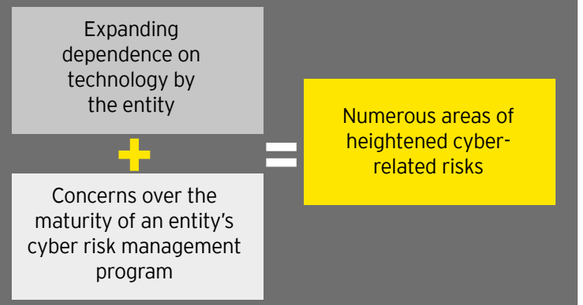
Benefits of taking action

- May prevent fraud, errors or financial reporting misstatements
- Creates an effective control framework
- May prevent deficiencies

Timing

- Mitigating controls can be implemented at year-end and impact analysis performed to confirm there was no effect on the financial statements despite the presence of SOD conflicts
- Controls should be in operation over the fiscal period

18 Is cyber risk given enough consideration in your risk management program?



Cyber risk

As the threat landscape rapidly changes and risks increase, companies need to change their mindset and approach toward information security and privacy to address a new normal. They need to operate under the assumption that unauthorized users are accessing the company's information technology environment on a daily basis – to assume "they're in."

Although not specific to your ICFR program, the assessment of cyber risk should be considered in any well-rounded risk management program. Organizations may have performed assessments of aspects of their security risks, but a comprehensive view of cybersecurity readiness may not be available within the organization. Meanwhile, investors, boards, media, customers, vendors and other stakeholders are asking questions.

The American Institute of Certified Public Accountants is considering guidance related to a new cyber risk management program attestation report, so you should stay abreast of new developments in this area. But when it comes to cyber risk, waiting is generally not a good answer under any circumstances.

Questions to consider

- Has your organization conducted a comprehensive cybersecurity assessment as part of the risk management program?
- Are your organization's policies and procedures up to date?
- Have you evaluated cybersecurity controls at your IT service providers?
- Has your organization incorporated cyber topics into the enterprise risk management (ERM) program?

Benefits of taking action

- May prevent breaches and operational problems
- Contributes to an effective risk management framework

Timing

- Controls should be in operation over the fiscal period
- Annual ERM activities may spearhead increased focus on controls around cyber threats
- Internal audits should be considered during planning and budgeting cycles

19 Have you considered how data analytics can help your organization evaluate controls and assess risks more efficiently?

15% of respondents indicated that data analytics is used to support the execution of ICFR programs

Data analytics

There is widespread recognition that automation frees up resources to be put to better use. By increasing your use of automated controls, you can drive down the number of manual touch points and labor-intensive detect controls in your processes. Similarly, using data analytics in the ICFR control testing process may have an effect on ICFR costs.

Data analytics continues to be an untapped resource by many compliance and internal audit functions. While some adoption has taken place, the sophistication of tools generally outpaces the funding and abilities of a company's internal functions to absorb and fully use them. The common areas of implementation are continuous controls monitoring in conjunction with systems; audit scoping to identify the highest-risk areas; and impact analysis in the case of identified control deficiencies.

While having in-house IA knowledge of technology generally makes operational sense, data analytics may be one area where a strategic partnership can yield better results. Access to tools and leading-practice experience should be brought to the table by your strategic partner to launch or refine the analytics program in support of your compliance efforts.

Questions to consider

- Does your organization have data analytics programs in place?
- Have you looked for additional areas that would benefit from ongoing analytical assessments?
- Have you evaluated manually intensive audit areas for opportunities to leverage data analytics?
- Have you considered whether data analytics can assist in the ICFR scoping process?

Benefits of taking action

- Covers a larger sample of the population and provides more differential focus on risks
- Identifies trends and all exceptions in a population
- Uses a more efficient audit approach

Timing

- When preparing for the annual ERM activities
- When asking for IA annual funding
- Ongoing

20 Does your organization leverage technology and tools to more effectively manage internal controls?

59% of survey respondents indicated that a tool, e.g., GRC, is used to maintain the documentation and testing of internal controls.

38% of survey respondents indicated a tool with built-in workflow functionality is used.

Leveraging technology and tools

Over the last 10 years, companies have continued to make significant investments in transaction processing technology. But adoption of full system capabilities and use of control and governance tools have not kept pace. Consider the following situations:

In some cases, the tools have been only partially implemented, e.g., the adoption of the user provisioning modules but not the business process control modules within GRC.

In other cases, technology tools used by IT groups have not been recognized and used as potential ICFR enablers. In that category are source code repository and release management tools, which can enable proper controls over changes to production systems and segregation of support vs. development duties. Also in that group is the use of commercial testing software, which enables implementation of a disciplined approach to financial system change testing and the gathering of testing and approval evidence.

Robust implementation of these tools and their inclusion in the risk and control frameworks reduce reliance on manual procedures and therefore reduce risk of control failures.

Questions to consider

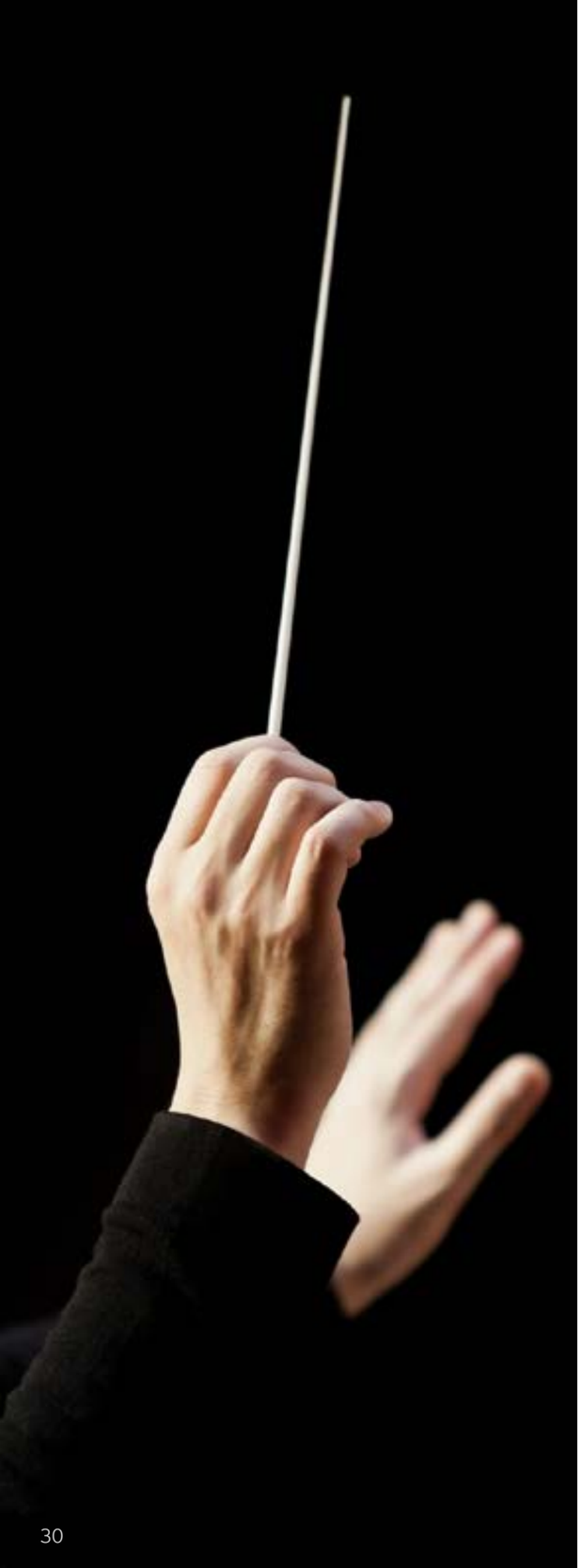
- Does your organization have the technology and tools to enhance the execution of internal control testing?
- Has your organization identified tools that would meet your requirements if not already in place?

Benefits of taking action

- Can allow companies to organize their procedures and more effectively and efficiently address risks
- May reduce overall cost of controls and minimize the level of employee effort

Timing

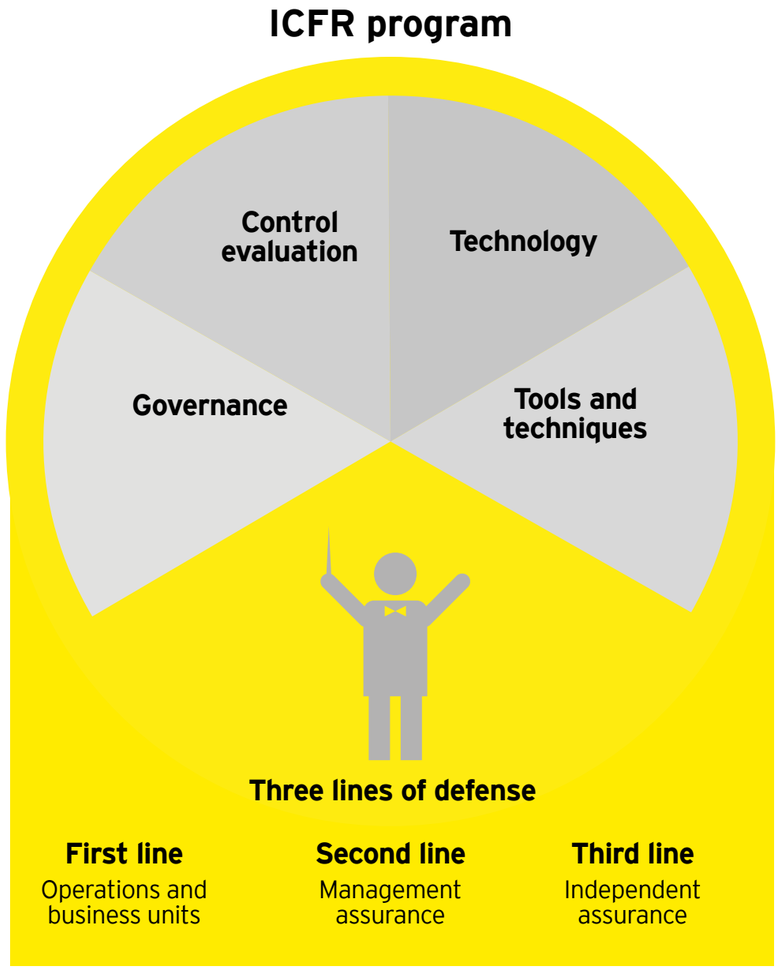
- Consider use of tools at the beginning of ICFR testing each year
- Ongoing



Refreshing your ICFR program can provide additional benefits

We know of no reason to expect that the velocity of change will slow down anytime soon. New players will enter the market with innovative ideas that will continue to disrupt business models, requiring companies to respond quickly to stay competitive. Technology will continue to rapidly evolve, upending the way companies do business and making them more vulnerable to "bad actors" looking for ways to infiltrate their systems. The ease of global communication through social and other media will continue to challenge organizations to stay on top of how they are perceived in the marketplace. And regulators will continue to evolve their requirements as they strive to protect stakeholders.

Re-evaluating your governance framework and ICFR program to determine whether they have kept up with the changes and making the necessary enhancements for what is known today are a good start. However, preparing for future changes is not a onetime effort or a compliance exercise. Rather, it is an opportunity to transform your organization's internal control governance structure and framework, resource model and use of technology to be more agile, efficient and effective. Additionally, it is an opportunity to clarify and reinforce the roles and responsibilities of the business, IT, internal audit and financial reporting functions to work together in harmony to help the organization meet its strategic objectives and improve business performance.



What can you do today to enact change?

- Be proactive about addressing emerging topics within your organization
- Revisit your governance structure and operating model for internal controls
- Collaborate with business and IT management on strengthening the control environment
- Refresh and enhance internal control documentation
- Evolve the nature, timing and extent of testing
- Use technology more extensively and creatively to become more efficient and effective
- Re-evaluate your staffing model and explore alternatives

To find out more about how our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or go to ey.com/advisory

Our Americas Risk leaders are:

Global Advisory Risk Leader		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
Americas Advisory Internal Audit Leader		
Lisa Hartkopf	+1 312 879 2226	lisa.hartkopf@ey.com
Americas Advisory Risk Assurance Leader		
James Martin	+1 216 583 3004	james.martin26@ey.com
Americas Advisory Region Risk Leaders		
Central		
Kevin Janes	+1 312 879 5400	kevin.janes@ey.com
Northeast		
Marcelo Bartholo	+1 215 448 2638	marcelo.bartholo@ey.com
Southeast		
AJ Desai	+1 704 331 1983	aj.desai@ey.com
Southwest		
Geoff Beatty	+1 713 750 1467	geoffrey.beatty@ey.com
West		
Scott Coolidge	+1 213 977 4206	scott.coolidge@ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

About EY's Advisory Services

In a world of unprecedented change, EY Advisory believes a better working world means solving big, complex industry issues and capitalizing on opportunities to help deliver outcomes that grow, optimize and protect clients' businesses.

Through a collaborative, industry-focused approach, EY Advisory combines a wealth of consulting capabilities — strategy, customer, finance, IT, supply chain, people and organizational change, program management and risk — with a complete understanding of a client's most complex issues and opportunities, such as digital disruption, innovation, analytics, cybersecurity, risk and transformation. EY Advisory's high-performance teams also draw on the breadth of EY's Assurance, Tax and Transaction Advisory Services professionals, as well as the organization's industry centers of excellence, to help clients deliver sustainable results.

True to EY's 150-year heritage in finance and risk, EY Advisory thinks about risk management when working on performance improvement, and performance improvement is top of mind when providing risk management services. EY Advisory also infuses analytics, cybersecurity and digital into every service offering.

The better the question. The better the answer. The better the world works.

With 40,000 consultants and industry professionals across more than 150 countries, we work with you to help address your most complex industry issues, from strategy to execution. To find out more about how our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view ey.com/advisory

1609-2070356

SCORE No. 00594-171US.

ED None

ey.com