



# Internal controls over financial reporting

**Outlining a program that meets  
stakeholder expectations**



After showing why a company's internal controls over financial reporting (ICOFR) program may be exposing it to more risk and/or higher costs than management realizes, this third in a series of white papers from KPMG's Risk Consulting practice looks at how to assess whether the ICOFR program is fulfilling its potential to benefit the company. Companies need to make strategic decisions for their ICOFR program to align with corporate objectives and meet key stakeholder expectations.













































# Don't be passive about ICOFR

Too many ICOFR programs obey two simple rules: (1) do the bare minimum to achieve compliance and/or (2) let the external auditor lead the way. But a just-enough-for-compliance approach will miss opportunities to support growth, mitigate risk, reduce costs, and drive value that ICOFR can provide. And the external auditor's priorities may not align with the company's objectives and needs.

Whatever approach companies take toward ICOFR, it shouldn't be a passive one. It should be a thoughtful decision based on what key stakeholders expect of the program.

To determine the right approach, the first step is to assess current performance by looking at the seven pillars (see Figure 1) of an ICOFR program.

**Figure 1: Characteristics of ICOFR program maturity**

Pillar	Lower Maturity	Higher Maturity
 <b>Strategy</b> Basic compliance driven	    	Value-driven culture
 <b>Risk assessment</b> Aged or unclear scoping	    	Identifies emerging issues
 <b>Entity-level controls (ELCs)</b> Undeveloped enterprise view	    	Integrates with enterprise
 <b>Control selection</b> Controls not aligned to business	    	Risk and control advisor
 <b>Testing strategy</b> Unclear or misaligned	    	Efficient and evolving
 <b>Evaluating results</b> Exception scorekeeper	    	Proactive management of root causes
 <b>Governance</b> Fragmented accountability	    	Innovative and aligned

# The seven pillars of a healthy ICFR program



## **Pillar #1: Strategy**

The foundation of every good ICFR program is a well-defined strategy that aligns with organizational priorities. That requires more than just focusing on the desired level of external auditor reliance. It requires understanding how that chosen level of reliance supports broader goals. More mature ICFR strategies aim beyond basic compliance—they support corporate values and strategies.



## **Pillar #2: Risk assessment**

An effective ICFR risk assessment connects key risks with audit assertions and supports the overall strategy, control selection, and testing approach. A more mature ICFR risk assessment isn't static. It's technology enabled, aligned with the enterprise risk assessment and includes qualitative risk factors so that it's more than just a financial scoping exercise.



## **Pillar #3: Entity-level controls**

Direct ELCs that operate at the right level of precision can act as an "insurance policy" to help mitigate other control failures if they occur. Management tends to shy away from ELCs due to external auditor concerns about precision levels and due to the requirements associated with management review controls. But, in practice, management often relies on direct ELCs to gain confidence in the overall financial results. It's wise to consider them in evaluating controls.



## **Pillar #4: Control selection**

Control selection should stay up to date with current business processes and focus on non-routine areas that require judgment. A common problem is too many key controls, many of which don't clearly link back to the overall assessment of financial reporting risk. The control inventory should include different kinds of controls (automated versus manual and preventative versus detective), contribute to improving control design and automation, and keep down the total cost of control.



## **Pillar #5: Testing strategy**

A healthy ICFR testing strategy adjusts the testing approach based on risk, incorporates continuous monitoring, and leverages management's knowledge and expertise.



## **Pillar #6: Evaluating results**

When ICFR runs smoothly, the results won't show many deficiencies. When deficiencies do occur, a mature program sets the right priorities: remediation efforts that implement sustainable solutions and also help improve operations and the broader organization. Without such robust remediation, which correctly identifies and completely addresses a deficiency's root cause, the deficiency may return in subsequent years—an all-too-common occurrence in many companies.



## **Pillar #7: Governance**

Good ICFR governance means the right tone at the top, frequent training for process owners and control testers, enough resources, and the right reporting structures. A mature ICFR program sets clear responsibilities and facilitates communication between who owns the overall program, who designs the controls, who performs the controls, and who tests the controls.



## The importance of assessing ICOFR program health

No company expects to find costly weaknesses in its ICOFR program, but companies that successfully signed ICOFR certifications one year may discover material weaknesses the next. Even programs without material weaknesses may still be spending too much, facing unnecessary risks, and failing to keep up with the rapidly changing demands on ICOFR.

The first paper in this series, ["Designing a healthy program that evolves to meet changing needs,"](#) outlines common causes of material weaknesses, Sarbanes-Oxley's (SOX) evolving demands, reasons ICOFR program health is important, and six questions to give companies an initial idea of the risks the program faces and the opportunities it may offer.

# Give the stakeholders what they expect

Once you've assessed how the ICOFR program currently measures on the seven pillars, it's time to determine what maturity levels the stakeholders expect and how the company will get there.

Not every ICOFR program needs to invest in achieving maximum maturity in every pillar. Part of meeting stakeholder expectations is making a strategic, risk-based, economic decision about ICOFR priorities. Some pillars will likely be functioning at a higher level of maturity than others. It may be worth investing more in some pillars. In others, it may be wise to accept certain minor risks in return for major cost savings.

What do stakeholders want from the ICOFR program? Common expectations include efforts to:



**Ensure** a strong 404a process



**Reduce** the impact of control issues



**Prevent** material weaknesses



**Develop** controls that enhance business performance



**Keep down** external auditor fees and the total cost of control



**Support** a company culture that drives improvements and efficiencies.

To help align the ICOFR program with the company's goals, objectives, and overall strategic direction, ask key stakeholders about their expectations. These stakeholders may include, among others:

- The Audit Committee
- The CFO and finance organization
- The controller's organization
- The CEO
- The CIO
- Internal audit and/or SOX team
- Owners of key processes.

What stakeholders say about their expectations will help determine how much to invest in the different pillars. It's often a good idea to add the external auditor on this list of stakeholders to see what they want most. But as we'll see, different regulations guide the company's needs and those of the external auditor. As a result, these two parties' needs don't always align.



# Add value by looking at the company's needs first—not the external auditor's

In KPMG's 2017 *Internal Controls Survey*, more than half of the respondents said their ICOFR program strategy is to ensure maximum reliance by the external auditor. In other words, they may be letting the external auditor dictate their ICOFR strategy. Sometimes management fears the external auditor will find an error, or they think reliance is the best way to reduce fees. But before a company makes maximizing external auditor reliance its goal, it should ask: have we set out a clear business case for this approach?

The ICOFR program should certainly consider the external auditor's needs, but they shouldn't be the only consideration. For a start, the external auditor has a different regulator than management: The Public Company Accounting Oversight Board (PCAOB) instead of the Securities and Exchange Commission (SEC). These two regulators have different demands and priorities (see Figure 2). And fundamentally, the external auditor has a different role than management: it has to come to an independent conclusion on both ICOFR and the company's financial statements.

When companies are less focused on external auditor reliance, they may have greater flexibility on documentation requirements and control testing. They can use the SEC's interpretative guidance and focus more on their own overall objectives.

**Figure 2: Reliance should be a deliberate economic decision**

Company's regulator			External auditor's regulator
SEC	Less auditor reliance	More auditor reliance	PCAOB
<ul style="list-style-type: none"> <li>— No requirement to update formal walkthroughs or flowcharts on an annual basis</li> <li>— Management's judgment plays a critical role in determining design of controls and how they are evidenced</li> <li>— More flexibility in determining how much to test and when</li> <li>— No sample size requirements</li> <li>— Completeness and accuracy should be considered by process owners when executing a control</li> </ul>	<ul style="list-style-type: none"> <li>— <b>Level of detail in process documentation</b></li> <li>— <b>More specificity around review controls</b></li> <li>— <b>More testing later in the year</b></li> <li>— <b>Depth of testing</b></li> <li>— <b>Completeness and accuracy testing</b></li> </ul>		<ul style="list-style-type: none"> <li>— Understand the flow of information through updated narrative/flowchart information</li> <li>— Level of precision, documentation around what attributes are reviewed for vis-à-vis expectations</li> <li>— Guidance around timing of testing (interim and rollforward) and sample sizes for each</li> <li>— Larger sample sizes, particularly for high-risk controls and test procedures that dig deep (via firms' methodologies)</li> <li>— Completeness and accuracy testing on all key spreadsheets and system-generated reports with stringent baseline approach or annual testing</li> </ul>



It may be the right decision to increase external auditor reliance, although that may require the company to invest time and money in moving up the scale to the PCAOB requirements. Such a move may (among other benefits) give management a good idea of what the external auditor will find when it tests. But it's also possible the extra effort needed to increase auditor reliance isn't the best use of a company's resources: its benefits may not outweigh its costs. Focusing less on external auditor reliance may open the door to other cost reduction strategies, such as smaller sample sizes or self-assessments in low-risk areas.

Either way, reliance should be a deliberate, economic decision. A company should determine its stakeholders' priorities, then engage in open dialogue with the auditor.



## Tips for effective coordination with the external auditor, regardless of the reliance strategy:

- Proactively discuss system, personnel, or process changes—and the corresponding impact on controls
- Consider ways to minimize impact on process/control owners (e.g., a central repository for control testing documentation, joint meetings, etc.)
- Understand both the PCAOB and SEC requirements for testing and evidence and how differences in requirements may impact differences in external auditor and management approaches
- Frame conversations regarding controls in terms of the risk assessment, what could go wrong and financial statement assertion
- Provide the external auditor the current control matrix and process documentation (e.g., narratives and flowcharts)
- Understand the population of controls being tested by the external auditor
- Strive for transparency around fees related to control testing and the impact of reliance on fees
- Communicate regularly regarding status and testing results

# The path forward

For an ICOFR program to fulfill its potential benefit to the company, it's better to pivot away from an exclusive focus on compliance and the external auditor's needs. It's also important to:

- Understand what your company's key stakeholders most expect from the ICOFR program
- Determine how well the program is currently meeting expectations in each program pillar
- Outline a roadmap to prioritize where the program needs to change to better meet expectations.

That roadmap should align with the company's overall ICOFR strategy and include a strong and effective financial statement risk assessment process—topics the fourth paper in this series will explore in depth.

With the right roadmap, a company will be on a path to ICOFR that not only fulfills compliance requirements, but also does what the key stakeholders most need it to—at a reasonable cost.



# Contact us

## **Bruce Willis**

**Partner & National Lead, Internal Audit, Risk & Compliance (IARCS)**

**T:** 306-791-1209

**E:** [brucewillis@kpmg.ca](mailto:brucewillis@kpmg.ca)

## **Heather Cheeseman**

**Partner, Internal Audit, Risk & Compliance (IARCS)**

**T:** 416-777-3314

**E:** [hcheeseman@kpmg.ca](mailto:hcheeseman@kpmg.ca)

## **Genevieve Leong**

**Partner, Internal Audit, Risk & Compliance (IARCS)**

**T:** 416-777-3226

**E:** [genevieveleong@kpmg.ca](mailto:genevieveleong@kpmg.ca)

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

[kpmg.ca/iarcs](https://kpmg.ca/iarcs)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2018 KPMG LLP, a Canadian limited liability partnership and member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.