Deloitte.

Refocus your risk assessment lens

Scale your ICFR program to focus on risks not benchmarks

Refocus your internal control lens

Transforming from a reactive to a proactive approach

Welcome to the first paper in the series, "Refocus your internal control lens: Transforming from a reactive to proactive approach." In this series, we'll be sharing our perspective on internal control over financial reporting (ICFR) areas. We'll also discuss frequently asked questions that present common challenges or areas of regulatory focus. We hope these insights can aid management in identifying opportunities to improve their system of ICFR.

We're keenly aware of the increasing focus the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB) are placing on ICFR, and we recognize the importance of ICFR to investors.

As Wesley R. Bricker, SEC chief accountant, stated in his December 5, 2016, keynote address before the 2016 American Institute of Certified Public Accountants (AICPA) Conference on Current SEC and PCAOB Developments:

> We are routinely reminded through our interactions with investors that they continue to believe that strong and effective internal controls and audits are an important component of the ability of companies to communicate credible financial reporting information in order to raise the capital needed to operate, grow and compete .... It is hard to think of an area more important than ICFR to our mission of providing high-quality financial information that investors can rely on. If left unidentified or unaddressed, ICFR deficiencies can lead to lower-quality financial reporting and ultimately higher financial reporting restatement rates and higher cost of capital.

In this first paper, we focus on an area we believe to be foundational to an effective ICFR system: the financial statement risk assessment that supports management's assessment under the requirements of Sarbanes Oxley Section 404a, or "SOX Risk Assessment."

Refocus your risk assessment lens

Scale your ICFR program to focus on risks not benchmarks

We're routinely asked about the size and scale of a company's ICFR program, with the primary focus on:

- Requests for industry peer group control count data to compare the number of controls tested by others as a benchmark to assess a company's own ICFR program.
- Requests to advise what controls can be removed from the ICFR program and still be "just enough" to earn a passing grade, as the perception that anything more is gold standard and unwanted.

Focusing on the control count as a benchmark metric for program sufficiency is a flawed approach, based on two key drivers:

- Variations in business models, organizational structure, use of technology, complexity, and operating environments—including regulatory—can result in different risks of error to the financial statements. Therefore, a different compliment of controls is necessary to mitigate risks.
- Variations in control count benchmark data, as each company's construct of controls differs. Differences may relate to aggregating multiple steps or attributes into one control versus having separate controls, selection of manual versus automated controls, or preventive versus detective controls, to name a few.

Unless the risk assessment details driving control selection and ultimate count are known and similar, the benchmarking data may not be meaningful. It could also be misleading for the company to use that data as an effective analysis comparison.

Start with a risk assessment

The starting point to evaluate the sufficiency of an ICFR program should be with a financial statement risk assessment. The risk assessment, which includes specific financial reporting objectives and identification of risks to achieving those objectives, answers these fundamental questions:

- Which controls are necessary to address the company's risks?
- How many controls does the company need?
- What is "just enough" for the company's ICFR program?

A risk assessment that integrates the right people, processes, tools, and techniques serves to identify the relevant risks of material misstatement ("ROMMs"). The risk assessment also includes the selection of controls and the evaluation of the design of the control in regard to the ROMM. It's through the risk assessment process that a company can report with confidence the number and types of controls necessary to have an effective ICFR system.

How do world-class organizations operate?

While the root causes of common risk assessment issues vary by company, we commonly see the following themes in effective internal control programs:

People

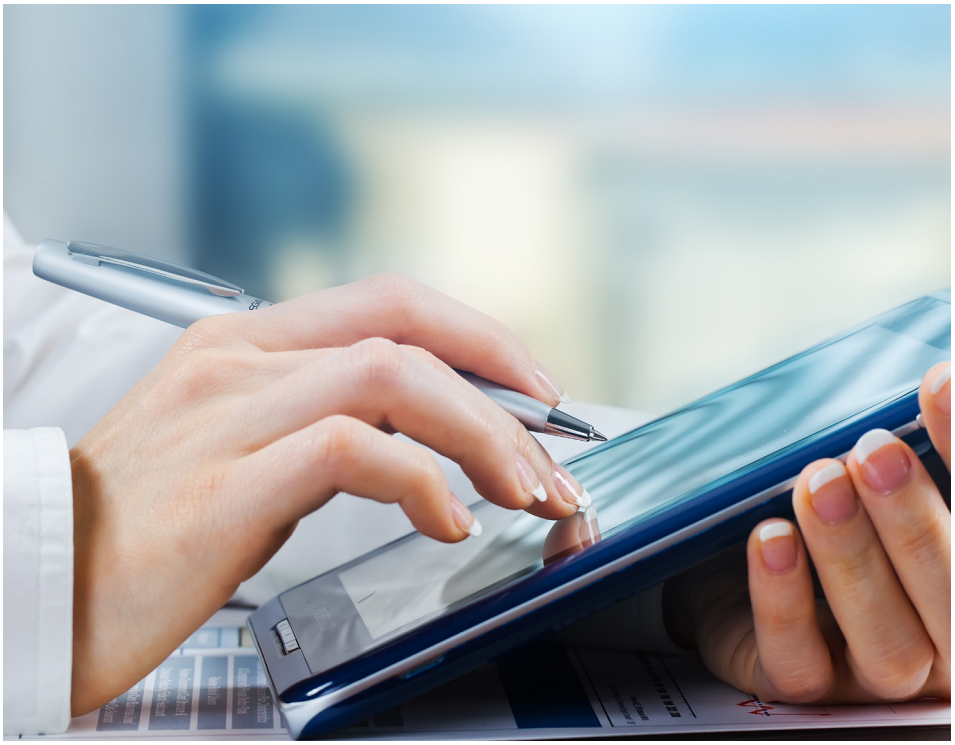
- The right people (i.e., cross-functional, multiple levels/divisions) with sufficient competency and knowledge contributing to the risk assessment process, including oversight.
- The internal control culture supports a risk-based approach, with risk ownership residing with management as the first line of defense. Refer to the Appendix for common issues in management's financial statement risk assessment process, which we view as potential contributors to material weaknesses and an ineffective and inefficient ICFR program.

Process

- A fully developed risk assessment methodology that's repeatable, documented, and performed at a sufficient level of disaggregation and granularity.
- The risk assessment is informed by the appropriate internal and/or external inputs, including, but not limited to, risk sensing techniques, or the use of third parties to provide specialized industry, regulatory, or innovative perspectives and insight when they don't exist internally.
- Internal programs are in place to inform those with risk assessment responsibilities of changes in the company where the impact of ROMMs should be assessed, especially around more complex areas, including non-routine transactions, fraud risk, cyber risks, and material weaknesses.

Tools and techniques

- The company utilizes innovative tools and techniques for performing and monitoring the risk assessment that results in value to the organization. (See the sidebar, "Data analytics and visualization tools," on page 4.)
- Automation of time-consuming spreadsheet analysis.
- Stress testing or war-gaming approaches are considered to challenge and examine the sufficiency of the controls in place to prevent or detect a material misstatement in a timely manner.



Is management missing an opportunity?

Companies that take a reactive approach to the risk assessment may be missing an opportunity to evolve, rightsize, and improve their ICFR programs while saving costs along the way.

The foundation of a company's ICFR program is built on risk assessments. Risk assessments should not be a reactive response to key stakeholders or performed only when issues materialize. Rather, management should proactively identify and assess new and existing risks. While the external auditors perform their own risk assessment process for the audit, the ability to align ROMMs and control selection can lead to a more efficient audit, as management and the external auditors should be closely aligned on scope, which provides more opportunities to leverage management's testing.

Risk assessments that are well-designed with the right people, processes, tools, and techniques can provide a customized, rightsized controls and related testing program based on responses to risks to support reliable financial reporting. Management should not need to look to external control benchmarks to compare and defend the size of their ICFR program, because they will have a solid documented basis to:

- Support their risk positions
- Elevate the visibility of risks to control performers and provide them with the information and tools needed to own their risks and identify mitigating controls in the most efficient and organizationally effective manner

Refocusing risk assessment through innovation

Companies can use the power of innovation in their ICFR program, including data analytics, process analytics, and visualization as part of the risk assessment process. This technique provides powerful insights that serve to inform the risk assessment process and help them hone what's truly a ROMM—at a more granular level—in order to vary the nature, timing, and extent of testing

based on risk. The result is typically a less costly and more effective ICFR program, which is grounded in a meaningful risk assessment.

With process analytics, management can take enormous amounts of data and repeatedly change the lens in which it's observed, providing valuable insight into the current state of operations. For example, effective use of process analytics can allow management to identify each class of transaction underlying a given account balance and then conduct a specific risk assessment for each, considering the following attributes[1]:

- Size and composition of the account
- Susceptibility to misstatement due to errors or fraud
- Volume of activity, complexity, and homogeneity of the individual transactions
- Nature of the account or disclosure
- Nature of the transactions—routine and automated or manual
- Whether judgment is utilized to record the transactions
- Accounting or reporting complexities associated with the class of transactions
- Exposure to losses
- Existence of related party transactions
- Changes from the prior period in account or disclosure characteristics

With this understanding, a company can assess the inherent risk for each class of transaction and conclude whether the risk of material misstatement is remote, lower, or higher. Then, based on this risk rating, the entity can vary the nature, timing, and extent of internal control testing to address the inherent risk for each class of transaction in an account balance or disclosure.

Next-gen controls

Many companies invest heavily in innovation, resulting in changes to key processes within the organization. Innovative activities, which can alter the organization's risk landscape and should be considered as part of an effective risk assessment, include:

- Reducing the number of processes, controls, applications, systems, tools, etc. that are in scope through consolidation, modernization, and risk assessment
- Centralizing systems, processes, technology, and people into fewer locations and support models (e.g., data centers, centers of excellence [CoEs], shared service centers, etc.)
- Standardizing and communizing configurations, processes, policies, controls, and procedures
- Automating the testing using tools (governance, risk, and compliance [GRC], utilities, scripts, etc.) and implementing automated controls leveraging system functionality where possible

Risk assessments that are well-designed with the right people, processes, tools, and techniques can provide a customized, rightsized controls and related testing program based on responses to risks to support reliable financial reporting.

[1] For additional examples of data analytics and visualization tools in use, see the sidebar, "Data analytics and visualization tools," on page 4.

Management can also challenge control selection to determine if the mix of control activity types is the most beneficial, considering resources and cost to the company. Entities can take advantage of innovative approaches, such as:

- More automated controls, which operate more consistently and effectively than manual controls
- Continuous monitoring controls, including the use of data and process analytics
- Robotics solutions for repetitive control activities to automate the testing of routine controls

Data analytics and visualization tools

As the surge of organizational and transactional data continues, conventional auditing approaches can't keep up with the information influx. Increasingly, financial and operational transactions are moving online, expanding the array of variables to analyze, outliers to identify, and trends and patterns to make sense of. Advanced audit analytics capabilities bring greater value to the audit process by supporting the analysis of large data sets and revealing more granular insights.

By enabling the analysis of entire sets of financial transactions, audit analytics aids in the interpretation and management of a growing storehouse of audit information. Audit analytics helps mine massive data sets to deliver smaller subsets of high-value data for the auditor to evaluate, improving both audit quality as well as the value of business insights an auditor is able to provide.

Figure 1-1: Overview of account balance totals year over year

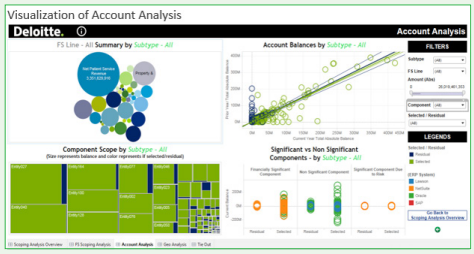


Figure 1-2: Changing the lens to see entity component balances by location

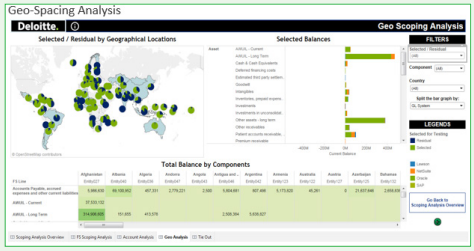
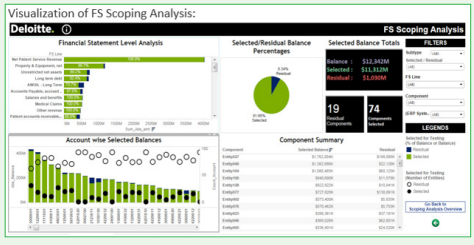


Figure 1-3: Financial statement line item coverage and residuals



The opportunities for value are derived from a reduction in compliance cost, a redirection of resources to focus on important business initiatives, and an increase in stakeholder confidence in the reliability of financial reporting, which ultimately may drive down the cost of capital.

As Wesley Bricker, SEC chief accountant recently stated, "Investors continue to believe that effective internal controls are an important component of the ability of companies to communicate credible financial reporting information to raise the capital needed to grow and compete."[2]

What can management do to refresh their lens?

As the SEC and PCAOB continue to increase their focus on ICFR, so should management. This focus should start with determining whether the company's risk assessment process is sufficient to identify and assess the risks to reliable financial reporting, including changes in those risks. Proactive steps management can consider include:

- Refreshing the risk assessment program to incorporate the right people, processes, and technologies to unlock the hidden value.
- Integrating data analytics and visualization to improve the quality of the data analyzed to support robust risk identification and report results succinctly to key stakeholders. This, in turn, can rationalize risks of material misstatement to a level of granularity to focus on what could truly be a material misstatement.

[2] Stated by Wesley R. Bricker, chief accountant of the Securities and Exchange Commission, in his December 5, 2016, keynote address before the 2016 American Institute of Certified Public Accountants (AICPA) Conference on Current SEC and PCAOB Developments.

Risk assessment diagnostic scorecard

The following scorecard includes some indicators that are meaningful in assessing the maturity of the SOX risk assessment process. "Yes," "somewhat," or "unsure" responses may be indicators that it's time to refocus your lens and refresh the SOX risk assessment process.

Indicators scorecard of a less mature SOX risk assessment	Yes	Somewhat	Unsure	No
Reporting indicators:				
Reported material weaknesses or significant deficiencies				
Control deficiencies – Inability to remediate or recurring deficiencies				
Material misstatements have occurred for which a risk of material misstatement wasn't previously identified				
SEC comment letters focusing on the identification of risks or other control matters				
Cultural indicators:				
Management, as the first line of defense, doesn't take ownership of risks and the identification of controls to mitigate risk. It relies on the SOX function, as the second line of defense, or the Internal Audit function, as the third line of defense, to identify risks, identify controls, and evaluate design.				
Management's approach to key stakeholders and external auditors is reactive versus proactive				
Process indicators:				
Failed ERP, reporting system, or IT-related implementations				
Issues within a process that results in delays in the deliverables for that process area, including reports or data submission relevant to financial reporting				
Accounting policies and procedures aren't updated on a periodic or timely basis to reflect changes in the company or changes in accounting standards				
Significant changes that may impact ICFR have occurred and weren't identified and assessed for potential ROMMs				
Tool and technology indicators:				
Tools and technologies used to support the risk assessment are highly manual				

Contacts

We want to hear from you. If you have questions or comments or would like to learn more about how innovation—such as risk sensing and visualization tools—can elevate and refresh your risk assessment process, contact one of our team members:

Patricia Salkin
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 732 890 6003
psalkin@deloitte.com

Amy Estrada
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 908 635 2914
amyestrada@deloitte.com

Todd Scarpino
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 908 337 2570
tscarpino@deloitte.com

Michael Corrao
Senior Manager | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
+1 714 436 7100
mcorrao@deloitte.com

Appendix

Common risk assessment issues

We believe that an insufficient risk assessment process is a contributing root cause to internal control issues cited in material weaknesses,[3] for example:

Internal control issue cited as a material weakness	Internal control issue as a percentage of total internal control issues reported in adverse opinions
Material and/or numerous auditor/year-end adjustments	19%
Information technology, software, security, and access issue	11%
Non-routine transaction control issues	6%

The common risk assessment issues identified below are potential contributors to material weaknesses and an inefficient and ineffective ICFR program.

Common risk assessment issues	Material weakness likely (i.e., ICFR isn't effective)
ROMMs go unidentified. Root causes include: • New risks not considered and/or periodically refreshed after a significant change impacting controls occurs within the company. • Risks not challenged based on approach and culture. • Lack of understanding and identification of applicable assertions.	• Management hasn't considered the ROMMs to support reliable financial reporting. • Appropriate control selection and design hasn't been considered in relation to the unidentified risks. Therefore, controls that should exist to address the ROMM may not exist or may not be designed to address the risk. • For example, non-routine transactions are scrutinized and assessed, with a focus on recording the transactions correctly. But management often doesn't assess the ROMMs, relevant assertions, and controls for financial reporting, disclosures, or cash flows. This has contributed to non-routine transactions being cited in 6 percent of reported material weaknesses for integrated filers in 2017.
ROMM identified, but the right control isn't selected to mitigate the risk.	• Risk mitigation is based on the design of the controls selected in regard to the ROMM. The appropriateness of the control to mitigate the risk is tested through design evaluation. If design testing isn't performed, then the company won't have assessed the appropriateness of the control selected to mitigate the risk. • Controls are selected to mitigate a risk; when design isn't tested, a possibility exists that the control doesn't mitigate the ROMM. • For example, in the warranty reserve scenario below, the granular ROMM more precisely articulates the true risk of material misstatement. Frequently, management is selecting controls that relate to period end account reconciliations or roll forwards, which may not focus on the review of the underlying inputs and assumptions that are found in a management review control.

[3] Material weakness data is based on a download from Audit Analytics as of July 11, 2017, for integrated filers. Source dates through July 5, 2017 – Data is limited to annual reports issued in 2017.

Common risk assessment issues	Material weakness likely (i.e., ICFR isn't effective)
IT risks weren't considered as part of the risk assessment process.	• IT risks can result in pervasive issues within ICFR, such as lapses in security, access, or change management. Cyber risks are pervasive IT risks that can affect all aspects of an entity, including financial reporting. • Control selection and design may not be focusing on the IT risk. Therefore, controls that should exist to address the IT risk may not exist or may not be designed to address the risk. • Lack of consideration of IT risks and control selection has contributed to information technology security and access issues being cited in 11 percent of reported material weaknesses for integrated filers in 2017. • An example of a common risk around change control is unauthorized changes being implemented into an IT system, due to lack of segregation of duties between individuals responsible for development of system changes and those responsible for implementation of those changes. Unauthorized changes could impact the functionality of the company's IT system, including incomplete or inaccurate data and/or processing.

Common risk assessment issues	Potential for material weakness (i.e., ICFR isn't effective)
ROMMs are identified, but not described at a sufficient level of granularity.	• When risks aren't described at a sufficient level of granularity, there's a risk that the relevant ROMM isn't identified and, therefore, is an unmitigated risk. • Control selection and design may not focus on the ROMM at the appropriate level. Therefore, controls that are selected to address the ROMM may not be designed to do so. • For example, a ROMM addressing the valuation assertion for a warranty accrual is noted as "accruals are subjective in nature and may be manipulated to project certain financial results" versus a more granular description of "the entity uses incorrect significant assumptions (e.g., historical claim rates and warranty periods) and underlying data (e.g., sales subject to warranty and historical repairs) to calculate and record warranty expenses." • The more granular risk will drive the level of precision in the management review control over the steps performed relating to the assumptions and data used that can address the risk.

Common risk assessment issues	Potential for material weakness (i.e., ICFR isn't effective)
ROMMS are identified, but no differentiation in the level of risk is stated (e.g., lower, higher, or significant).	• In this case, resources are dedicated without consideration to level of risk, resulting in the performance of procedures that may be inconsistent with or insufficient for the level of risk. • For example, an entity challenged the risk level of a ROMM by performing a top-down approach for a material flow of transactions that's highly automated, concluding that a previously identified normal risk is a lower risk. The top-down approach included procedures to consider: – The entity and its environment, including internal control – Results from past audits and internal control testing – Preliminary analytic procedures – Discussion with management and others • As a result, the entity was able to reduce the extent of testing by reducing the testing sample sizes for the control and varying the nature of testing.
A risk assessment framework or methodology hasn't been developed or is ineffective, as a basis to perform the risk assessment.	• If the organization lacks an effectively designed risk assessment program, this may indicate that one or more of the COSO risk assessment principles aren't present and functioning, which would result in a material weakness in the principle and the risk assessment component. • Leading practice organizations have a documented framework and utilize innovative tools and techniques to analyze and report risk assessment results. • Examples of leading practice tools include: – Data analytics to identify trends and analyze populations – Visualization tools to provide deeper insights and enhanced business analysis – Modeling tools that examine a wide range of industry data and predict potential risks using trend and regression analysis

Common risk assessment issues	Minimal risk of material weakness (i.e., ICFR is still effective)
ROMMs are identified, but are incorrectly assessed as potential material misstatements when they are not.	• In this case, resources are dedicated to an area that isn't material. • Controls are selected and evaluated for design that don't relate to a ROMM. • For example, an entity is in the last year of a restructuring program, where the remaining program costs are immaterial to the financial statements, but the entity continues to identify ROMMs associated with the program and test-related controls. An example ROMM within the program is the valuation of severance liabilities, all of which have been paid, except for an immaterial amount for the remaining program year. Therefore, those controls associated with that ROMM shouldn't be formally tested and evaluated in the current year program.
Control selection isn't challenged to determine if the mix of control activity types is the most beneficial, considering resources and cost, to the company.	• There may be other controls with appropriate control design to mitigate the risk that may be more efficient to test. • Control selection can be tailored to consider the: – Nature of the control – Manual or automated – Approach – Preventive or detective – Type – Verifications, authorizations and approvals, physical controls and counts, reconciliations, controls over information used in a control, and management review controls • For example, many entities may not be taking advantage of the following in new or existing systems: – Automated controls – Continuous monitoring controls, including the use of data analytics – Automating spreadsheets into a system-generated report – Robotics solutions for repetitive control activities

Deloitte.