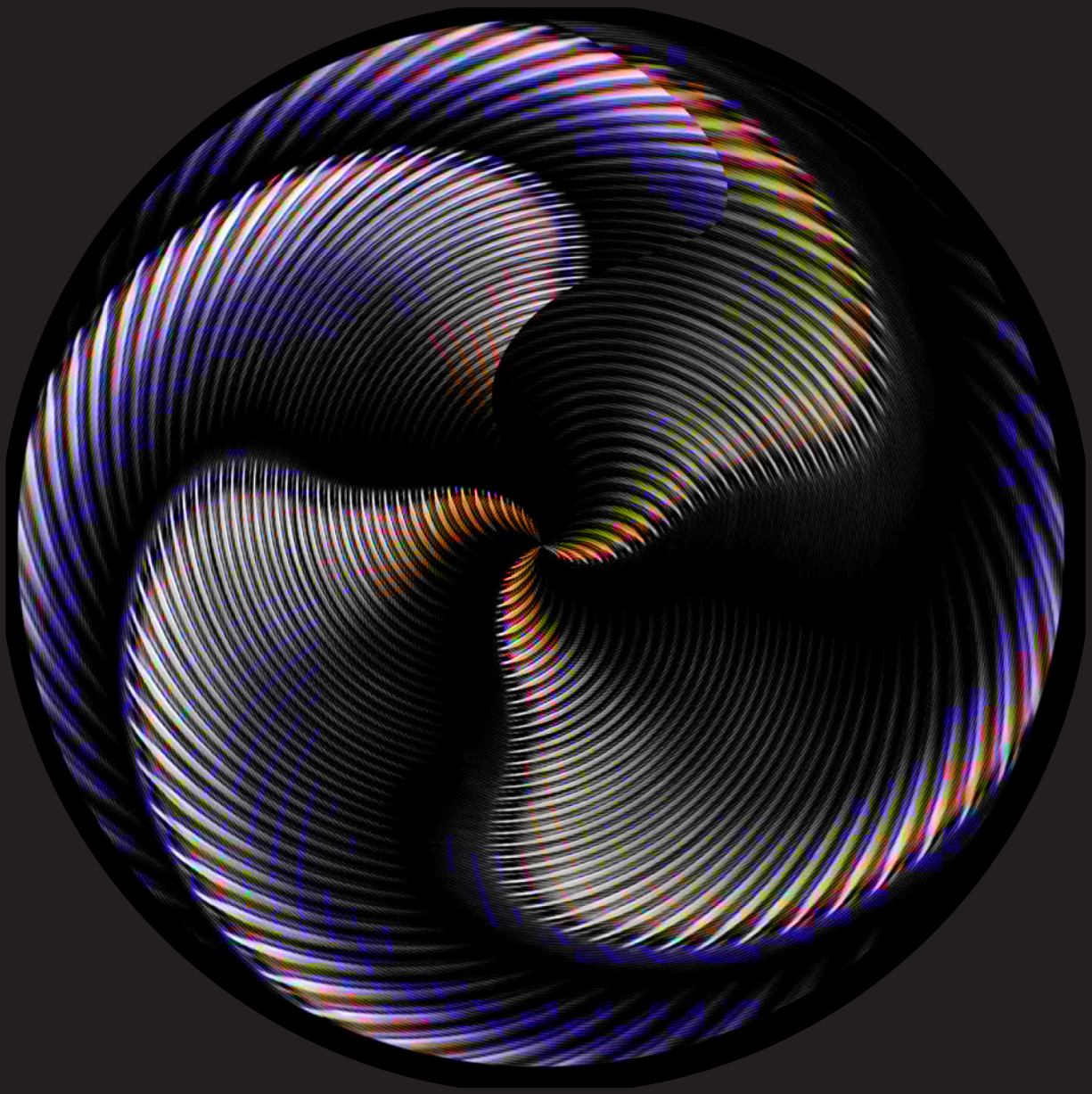
Deloitte.



Refocus your 302 certification programs lens

How to unlock hidden value

Contents

Refocus your 302 certification programs lens

How to unlock hidden value

The Sarbanes-Oxley Act of 2002 (the Act or SOX), most commonly known for the annual internal control requirements of Section 404, also includes specific requirements related to the periodic financial statements within Section 302, also known as the "302 certification."

When organizations initially are required to comply with Section 302, they frequently ask questions related to the 302 certification, such as:

- Who should certify, beyond the certifying officers?
- What should they certify to?
- Who should evaluate changes reported?
- What should the assessment for significant change for required disclosure consider?
- What technology is available to automate the certification process?

Organizations seldom reconsider how they initially structured their 302 compliance process (302 program). As such, few ever ask, "Can we optimize the 302 certification process to unlock hidden value to identify organizational efficiencies, enhance quality, and lower the cost of compliance?"

We have a perspective on that unasked question, and we believe the answer is yes. We will share our perspective on areas where hidden value can be extracted.

Background

Section 404(a) of SOX can be summarized as requiring management to perform an annual assessment of the effectiveness of internal controls over financial reporting (ICFR) as of the organization's year-end date and to present its assertion as to the effectiveness of the organization's ICFR (SOX 404 program). This assertion in an issuer's first annual Form 10-K, required by the Securities and Exchange Commission (SEC), including management's assessment under 404a filing, serves as a baseline for Section 302 quarterly requirements. Subsequent to the first annual Form 10-K, Section 302 quarterly certifications require the establishment, maintenance, and design of internal controls (302(a)(4)(A) and 302(a)(4)(B)). (The requirements for Section 302 are included in Appendix A. Refer to Appendix B for the ICFR requirements timeline.)

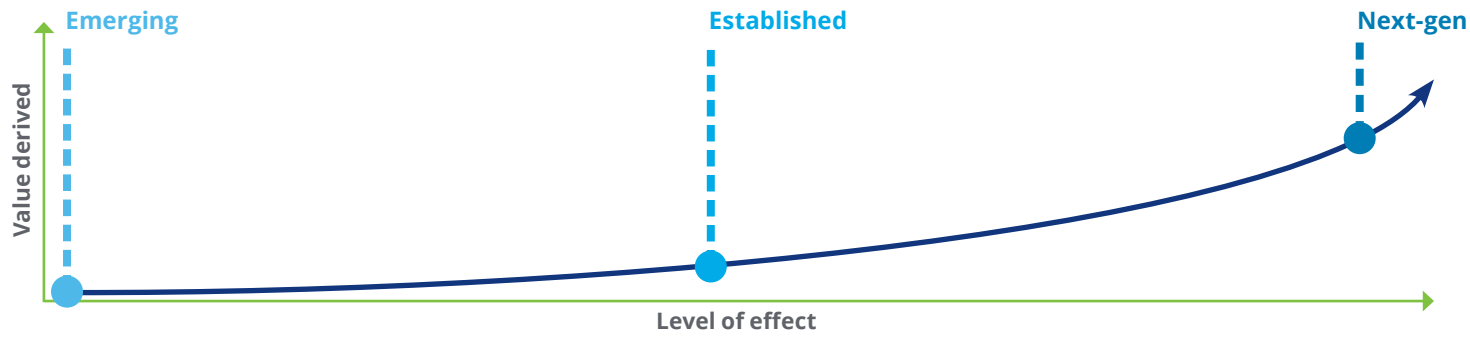
The design of a 302 program will vary across organizations, with considerations including the size, structure, global footprint, culture, and technology capabilities. Two other factors that may affect the design of the 302 certification program are 1) where an organization lies on the maturity model (table 1) and 2) its desire to unlock hidden value.

Hidden value unlocked

Organizations that view the Section 302 requirements as a burden or a check-the-box exercise are likely missing opportunities to unlock hidden value, which may have a broader impact on a system of internal control. We have identified tenets of a strong 302 program, enabling hidden value to be extracted in the form of increased efficiencies between 302 programs and SOX 404 programs, integration of other objectives, improvements in the quality of controls, and/or reductions in the overall cost of compliance.

The following illustrates the level of effort required to extract hidden value from 302 programs. We have found that many organizations have established the minimum requirements for their 302 program without consideration of the possibility to unlock hidden value from the effort of compliance they have undertaken. With minimal investments in the process, heightened accountability, greater sense of ownership, and more efficient information-gathering can be some of the simplest returns on investment. When highly optimized, even more information is gathered with greater transparency and accountability, while the process is truly streamlined, scalable, and automated to minimize impact on the organization.

Table 1.



	Emerging	Next-gen
Governance	• Certification ownership, authority, accountability are not established or clear • Minimal tone at the top regarding certification	• Certification ownership, authority, accountability are embraced by the organization • There is clear accountability and ownership for certifications • Strong tone at the top regarding certifications
People	• Only CEO and CFO certifying or limited number of individuals certifiying • No or limited organization-wide representation	• Certifiers range from CEO and CFO down to control owners • Organization-wide representation
Process	• Limited infrastructure supporting certifications • Certifications rely on implicit processes (such as 404 Program testing) as opposed to activity explicitly designed to identify changes in the control environment • Not all changes (such as outside service providers or systems) are considered	• Strong infrastructure supporting certifications • Various assessment activities are integrated in the certification process • All changes are considered and control owners own the maintenance of their control documentation • The results of the certification process are factored into ongoing risk assessment activities
Tools and technology	• Heavy reliance on manual processes • Limited use of workflow capabilities • No integration between periodic assessment data and certification process	• Integration with governance, risk, and compliance (GRC) tool, utilizing workflow capabilities and seamless integration between periodic assessment data and certfication process

"How many sub-certifiers?" This is a common follow-up question, but asking yourself "Who?" is perhaps even more important. As risks that affect financial reporting and internal controls may reside throughout the organization, not just within finance and accounting, sub-certifiers from other parts of the organization should be represented as well. Insights from internal audit, information and technology, operations, human resources, legal and compliance, and others may be necessary to capture a complete inventory of those items warranting attention from the principal executive and financial officers (CEO and CFO) (Figure 1).

- As information that is evaluated as part of an organization's 302 program will extend throughout numerous departments and levels of management, it remains critical to have the right individuals providing oversight of this process.
- Establish a sense of ownership among sub-certifiers such that they effectively communicate and appropriately escalate issues or changes affecting the business and technology environments.

Below, we have laid out common challenges and leading practices relative to each of the dimensions—governance, people, process, technology, and tools—of a 302 program.

Governance

Common challenge:

Lack of ownership by management more broadly (for example, business leads, process owners, and control owners) as the first line of defense (LOD) for ICFR responsibilities

Leading practice consideration:

Drive accountability by designing 302 sub-certifications, which support 302 programs (refer to Appendix B for illustrative questions), with the following elements:

- Sub-certify at the business process and control level
- Sub-certify that changes in process or controls have been updated in control documentation (such as process flow diagrams, narratives, and written control descriptions) as of quarter-end
- A sub-certification program—certifying officers rely upon a series of sub-certifications occurring at subordinate levels within the organization, which can serve to promote accountability, ownership for risks and controls, and timely reporting
- A strong tone at the top conveying to sub-certifiers that the effort is not a check-the-box exercise
- Training and communication to align objectives, roles, and responsibilities
- Annual testing of the 302 program to conclude on the design and operating effectiveness

People

Common challenge:

Difficulty identifying sub-certifiers beyond the CEO, CFO, and disclosure committee members related to the additional parties involved in the 302 program

Leading practice consideration:

Characteristics of potential sub-certifiers may include:

- People with knowledge of the health of the system of internal control
- Enough people who can speak to the broader organization as it relates to financial statements

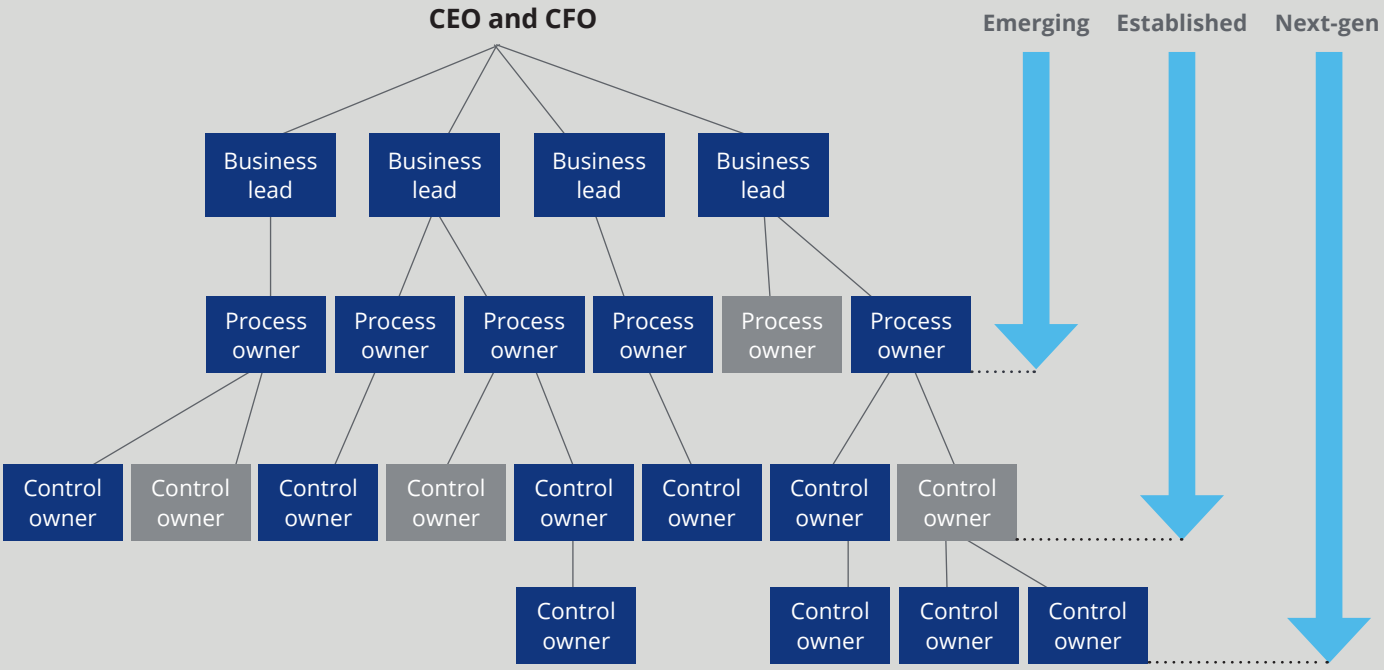
Additionally, a group to help coordinate and liaise with sub-certifiers and triage potentially concerning responses before sharing with the next level of sub-certifiers is typically necessary.

Sub-certifiers should be sub-certifying to, among other things:

- The results of the design and operations of controls to allow for the assessment of disclosure impact
- Matters that, while not significant, may have an impact on ICFR

Figure 1.

The following is an illustrative example of the levels of sub-certifications at each of the maturity levels. A truly optimized 302 program includes multiple sub-certifications, allowing for greater transparency and accountability.



Employees completing sub-certifications

- Employees that will complete sub-certifications for ICFR controls
- Employees that will complete sub-certifications for non-ICFR areas that may still require disclosure (such as cyber)

Process

Common challenge:

302 sub-certifications are not typically designed and/or leveraged with the intention to harmonize various requirements relative to the three objectives of the Committee of Sponsoring Organizations of the Treadway Commission (COSO): operations, reporting, and compliance.

Leading practice considerations:

Leading practice considerations promote the following outcomes for 302 programs and/or other requirements:

- **Reduce extent of rollforward testing as part of SOX 404 program requirements.** Organizations may utilize a quarterly sub-certification process to support the required 302 certifications in quarterly filings with the SEC and to identify material changes in ICFR. Management may also view this process as an ongoing monitoring activity intended to determine whether changes have occurred that are relevant to ICFR and to support conclusions about whether the relevant underlying controls have continued to operate effectively. For example, if the purpose of the sub-certifications is to identify changes in the effectiveness of the design and operation of relevant controls, then the sub-certification may be deemed an effective monitoring control, which can serve to reduce the extent of rollforward testing. If the purpose of sub-certifications, however, is not to explicitly identify changes in the effectiveness of relevant controls, it is unlikely this monitoring activity will be sufficient for purposes of serving as a rollforward procedure (for example, minimizing additional operating effectiveness testing).

- **Eliminate the need for annual walkthroughs for processes operating at a steady state.** Additionally, an effective sub-certification process may enable an organization to help assess the steady state of processes to potentially eliminate the need for annual walkthroughs to inform the risk assessment process, both annual and ongoing. An effective sub-certification process that identifies changes that may affect ICFR enables early response and the ability to test, in a timely manner, changes that are deemed higher-risk.
- **Identify and monitor outsourced service providers (OSPs).** Organization may also utilize 302 programs to identify new OSPs and/or monitor existing OSPs.
- **Monitor requirements for other regulations that may have controls monitoring requirements.** Enhancements to existing 302 programs may be incorporated to monitor requirements for other regulations by designing specific questions for select individuals, with responses routed to the appropriate parties for review (refer to Appendix B for illustrative questions relative to cyber and SEC Rule 17a-5).
- **Elevate awareness and accountability for cybersecurity.** Utilize the sub-certifications as a means to elevate awareness and accountability for cybersecurity matters by designing specific sub-certifications to those who have roles and responsibility or access to sensitive information such as personnel, customer, or vendor data. Upon identification of cybersecurity risks and incidents through the 302 program, escalate matters for further assessment and to determine if disclosure is required. Direct all cybersecurity responses to the appropriate party for assessment of results on a quarterly basis.
- **Create a sustainable program** that is fit for purpose. Creating a program that is overengineered will likely result in it falling under its own weight. Similarly, creating a program that is a check-the-box exercise will not benefit the organization.
  - Frequently, the sub-certification process will require sub-certifiers to perform a certain degree of diligence (for example, helping to ensure internal control documentation is updated, identifying relevant changes to risks or controls, and assessing the ongoing design and operating effectiveness of controls) so sub-certifications are supported by a deeper diligence.
  - The recurring nature of Section 302 also provides an opportunity for communicating additional internal control and financial reporting topics to sub-certifiers (such as new accounting guidance, training reminders, or other key points management wishes to convey) through updates to the sub-certification questions.

Tools and technology

Common challenge:

Modernization of a 302 program through tools and technology simplifies what is often a highly manual program so that less time is spent on dissemination and compilation.

Leading practice consideration:

Leading practices include:

- Survey tools to streamline the dissemination and aggregation of responses
- Automated workflow capabilities to route assignment of 302 sub-certifications to people based on their roles and responsibilities and track responses
- Automated reporting of results, including extraction of matters requiring further review
- Data visualization tools to facilitate dashboard reporting and/or trend analysis
- GRC tools may capture design and operating effectiveness assessment procedures and results and link them to sub-certification questionnaires

Integrating technology serves to drive efficiencies in the execution of the sub-certification process and improve the reporting to senior stakeholders. Technology enables certifiers within larger and more complex organizations to obtain the same level of comfort that their counterparts may achieve at smaller and flatter organizations.

302 programs may facilitate the identification, summary, and evaluation of information for which formal disclosure controls and procedure change committees are being tasked with oversight. These committees may be enhanced by assuming responsibilities for emerging topics, such as cybersecurity breaches and related controls. In particular, the Division of Corporation Finance issued guidance in 2018[1] reinforcing previously issued 2011 guidance[2] emphasizing the need to establish and maintain appropriate and effective disclosure controls and procedures that enable companies to make accurate and timely disclosures of material events, including those related to cybersecurity. Disclosure committees may serve as an effective way of monitoring for the need for added disclosures (such as cybersecurity events).

What do you do when an item is reported as part of the sub-certification process?

There is no one-size-fits-all answer. The criteria to evaluate may vary by organization, based on the complexity of the organizational structure. Considerations we have observed include:

- An assessment of the impact on, or pervasiveness of change to, the financial statements and disclosures, the governance structure, people, processes, and technology, performed by people in the organization with knowledge of the affected area and the correlation of such to ICFR
- An assessment of whether potential deficiencies were previously reported and assessed or need to be evaluated
- Timing considerations (for example, how long will the change affect the organization?)

For all potentially significant changes, management should document their considerations and basis for conclusion regarding the need to disclose or not. Commonly disclosed significant changes for financial reporting in SEC filings include:

- Remediation of material weaknesses
- Significant IT implementations

For changes that do not elevate to the level of significance for financial reporting disclosure, the changes should be assessed for the impact of changes on ICFR, considering materiality and financial reporting objectives. For example:

- Refresh risk assessment and control selection
- Consider impact of change on annual SOX 404 program testing plan
- Consider impact of change on the organization and the need to update training and control documentation

It is important to note that disclosure of a significant change in internal control should not only occur in the period when the change occurs, but should also originate when the significant change becomes known and would be considered relevant to the users of quarterly financial statements. For example, the implementation of an organization-wide ERP system may occur over multiple quarters (or even years), and disclosure should occur when the change has been initiated, as opposed to completed.

A matter of trust—or trust, but verify?

A common question is "what repercussions exist for the CEO and CFO related to ineffective 302 programs?"

The SEC Enforcement Division can bring charges against a CEO or CFO when there is material noncompliance with financial reporting requirements due to misconduct by the organization, or by the executives, including false certifications under Section 302. Enforcement actions can include sanctions, such as:

- Reimbursing the organization for any bonuses and incentive-based pay or profits from the sale of stock received in the twelve months prior to an earning restatement (often referred to as the clawback provision under Section 304)
- Paying civil penalties
- Being barred from serving as an officer of a publicly traded organization for a specified period
- Suspension for a period from practicing as an accountant of any publicly traded organization, or any organization regulated by the SEC
- Cease and desist against further violations

In 2011, the SEC released disclosure guidance[3] related to cybersecurity, which outlined the requirements for disclosing risks and cyber incidents. Cybersecurity continues to be a hot topic among boards and investors, as noted by the SEC's release in February 2018 of interpretive guidance[4] to assist public companies in preparing disclosure about cybersecurity risks and incidents, as well as current SEC chairman Jay Clayton's comments:

"In today's environment, cybersecurity is critical to the operations of companies and our markets. Companies increasingly rely on and are exposed to digital technology as they conduct their business operations and engage with their customers, business partners, and other constituencies. This reliance on and exposure to our digitally connected world presents ongoing risks and threats of cybersecurity incidents for all companies, including public companies regulated by the Commission. Public companies must stay focused on these issues and take all required action to inform investors about material cybersecurity risks and incidents in a timely fashion."[5]

Unlock hidden value through next-gen certification

Organizations have an opportunity to unlock hidden value through next-gen certifications, especially those organizations that have highly manual 302 programs or minimal sub-certifiers, or that have not refreshed in many years.

Management can develop a next-gen certification program by challenging the current governance, people, processes, and technology, as well as by identifying the areas within its organization where hidden value may exist.

Contact us. We are here to help.

Contacts

Patricia J. Salkin
Managing Director | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 609 806 7279
psalkin@deloitte.com

Adam Berman
Partner | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 212 436 7267
aberman@deloitte.com

Stuart Rubin
Managing Director | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 561 962 7826
stuartrubin@deloitte.com

Matt Tilner
Senior Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 212 492 4281
mtilner@deloitte.com

With special thanks to Jeff Aughton, Michael Corrao, Chris Decker, Divya Mathew, Stefan Ozer, Hayden Stone, Sandra Teixeira, and Craig Weibman.

Endnotes

1. US Securities and Exchange Commission (SEC), Division of Corporation Finance, *17 CFR Parts 229 and 249: Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, February 26, 2018, https://www.sec.gov/rules/interp/2018/33-10459.pdf.
2. SEC, Division of Corporation Finance, "CF Disclosure Guidance: Topic No. 2," October 2011, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
3. Ibid.
4. SEC, 17 CFR Parts 229 and 249.
5. SEC, "Statement on Cybersecurity Interpretive Guidance," press release, February 21, 2018, https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21.
6. SEC, 17 CFR Parts 228, 229, 232, 240, 249, 270, and 274. SEC, [RELEASE NOS. 33-8124, 34-46427, IC-25722; File No. S7-21-02], https://www.sec.gov/rules/final/33-8124.htm.
7. Title 17: Commodity and Securities Exchanges, Part 240—General Rules and Regulations, Securities Exhange Act of 1934, https://www.ecfr.gov/cgi-bin/text-idx?SID=30da76ab97612d5b10ba77694a2c0628&mc=true&node=se17.4.240_113a_614&rgn=div8.

Appendices

Appendix A

Section 302 requirements:[6]

- 302(a)(1) – The signing officer has reviewed the report.
- 302(a)(2) – Based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading.
- 302(a)(3) – Based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report.
- 302(a)(4)(A) – The signing officers are responsible for establishing and maintaining internal controls.
- 302(a)(4)(B) – The signing officers have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared.
- 302(a)(4)(C) – The signing officers have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report.
- 302(a)(5)(A) – The signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls.
- 302(a)(5)(B) – The signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls.
- 302(a)(6) – The signing officers have indicated in the report whether or not there were significant changes in internal controls or other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

Appendix B

Identifying potential changes to internal controls.

While the requirements for disclosure only include those changes that are considered "significant," the identification of these potentially significant changes may come from almost anywhere within the organization. "What should we consider?" is the usual question, and while there is no prescriptive list issued as part of Section 302, management may consider the following illustrative questions for each of the potential sub-certification levels:

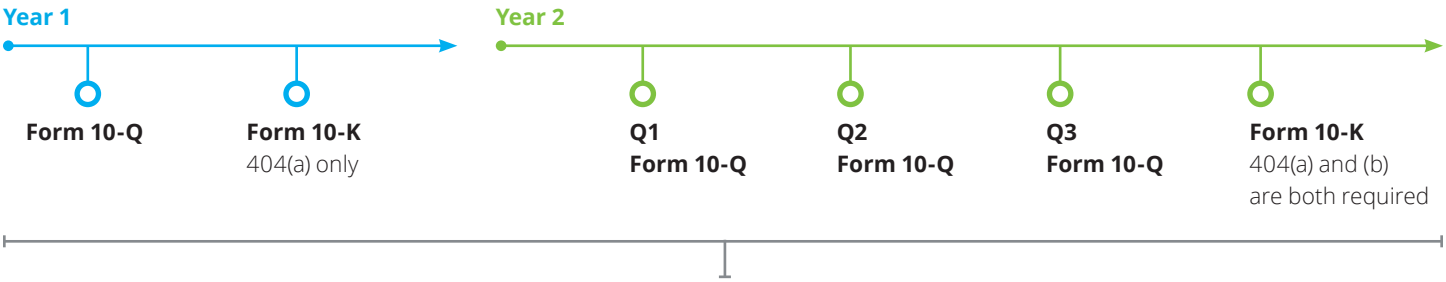
		Potential sub-certification levels			
Area	**Example sub-certification questionnaire**	**Business lead**	**Business process owner**	**Control owner**	**Outside service provider or relationship owner**
Risk assessment	Have there been any significant changes made to business processes, procedures, or control activities?	✓	✓	✓	✓
Controls	Have there been any changes in the control design during the quarter? For example: - Control owner - Frequency - Control steps - Information used in the control (such as reports or data) - Configurable settings		✓	✓	✓
Controls	Have there been any deviations in the performance of the control during the quarter? For example: - Control not performed - Control performed, but not documented - Control not performed timely, waiver not obtained		✓	✓	✓
Personnel	Have there been changes in key personnel involved in SOX 404 program controls and financial reporting roles?	✓	✓	✓	✓
Outsource service provider (OSP)	Have there been changes to the OSPs' (third parties that provide services on behalf of management involving transactions related to internal controls over financial reporting) scope of services?	✓	✓	✓	
Related parties	Are you aware of any new related-party transactions (for example, transactions with any employee, director, or 5 percent or greater stockholder, or their family members or relatives) entered into during the current period? If so, please provide the name of the related party, nature of relationship, and approximate value of transactions that have and/or will continue to take place with this related party. *For purposes of this question, a related-party transaction does not include amounts paid to an employee or director for service in such capacities.*	✓	✓		
Cybersecurity	Are you aware of any inappropriate release of confidential information to either internal or external parties that was not communicated timely to the appropriate privacy officer or business unit management?	✓	✓	✓	✓
FINRA Rule 17a-5	Have there been any significant changes to end-user computing tools or key reports that support the reserve formula and the net capital computation?		✓	✓	

Appendix C

ICFR requirements timeline post–initial public offering

The majority of this document makes reference to how organizations with established 302 programs can make enhancements to extract hidden value. New issuers may leverage lessons learned from more established organizations to avoid previously encountered common challenges and accelerate to leading practices.

The chart below depicts the sequence of events from an organization's initial public offering through the issuer becoming subject to ICFR requirements in their second Form 10-K.[7]



302 is required; however, the chief executive officer (CEO) and chief financial officer (CFO) may omit the portion of the introductory language in paragraph 4, as well as language in paragraph 4(b) of the certification (responsibility for designing, establishing, and maintaining internal control over financial reporting)[7]

In order to meet the requirement of Section 302, organizations generally leverage a quarterly certification process to provide a basis to update the annual baseline reported under Section 404.

Deloitte.