Deloitte.

Center for Controllership™

Don’t lose control of your internal controls program

Frequently asked questions about risks and controls in a time of crisis

What are some considerations for a remote workforce to remember when performing internal controls over financial reporting (ICFR)? How does COVID-19 affect tax reporting? What can you do to prepare for a potential crisis in the future? As many organizations find themselves performing internal controls, conducting reviews, and reporting taxes in a remote work environment, here are some frequently asked questions professionals may have as they navigate risk and controls in a crisis.

Governance

Q. With the overnight change in my working location, how do I keep our Controllership organization on track with month-end and quarter-end close?

A. Now more than ever, there is a need for coordination and organization. Some clients are leveraging close checklists, adding more detailed steps and defining owners with clear backup owners. It is also helpful to empower one leader to own the overall checklist who can monitor the timely completion of each activity. Also, don’t be afraid to go heavier on daily check-ins during the busy days of close. These can be brief, 15-minute virtual sessions to discuss the priorities for that day and see if there are any risks that would prevent completion.

Q. How do we prepare for virtual controls walkthroughs?

A. When initiating a virtual walkthrough, specifically as it relates to the use of technology, the parties involved may want to consider preparing in advance by confirming the selected technology is working appropriately for all participants and inquire if the control owner(s) has/have the ability to share their screen during the walkthrough.

Viewing and evidencing information when conducting a virtual walkthrough may deviate from normal circumstances. Methods are going to be new to many participants, so the following are examples of considerations when preparing for the walkthrough:

- Request and collect any information expected to assist in facilitating the discussion in advance of the walkthrough, such that it is available for review or reference during the walkthrough
- Verify all pertinent information (such as dates, parameters, and evidence of review) referred to during the walkthrough is visible
- Obtain necessary screenshots or evidence to be provided after the walkthrough to validate the information that participants observed

Q. What advice do you have for organizations that are less technologically savvy?

A. Without a doubt, there will be companies that are on both ends of the spectrum when it comes to technology adoption and maturity. For those that have already taken steps to automate their controls and leverage a governance, risk, and compliance (GRC) solution to manage their SOX 302 and 404 processes, there will likely be less organizational change management. For those companies that are either just beginning to implement or just beginning to strategize how to effectively leverage technology, this situation can really be a catalyst to take the next step in the journey. Understanding the impact to the control environment—specifically what manual controls are in place that may be difficult to execute remotely or the business changes that enable a need for a full redesign—can be crucial data points to justify to C-suite executives or boards of directors that now is an opportune time to invest in technology. Technology enablement reaches beyond the control environment, and when taken into consideration with how technology can automate end-to-end processes, the business case may be compelling. To make it more manageable, consider starting small with a rapid controls impact assessment to understand where there are opportunities to automate. Combine that with a swift technology assessment to understand what applications and solutions you have within your current environment that may be enhanced to maximize automation capabilities. These starting points can provide key data on where to focus first as you build your longer-term roadmap to technology enablement.

Q. I was just delegated as a key control owner, and this will be my first time executing this manual control; what type of training and onboarding documents should I be leveraging?

A. If the primary owner is available for a brief transition conversation, take advantage of that opportunity to understand how the control operates, its intent, and what objective(s) it addresses. Knowing the context of the risk that a control is mapped to is vital to understand what components of the review are key. Assuming this is a manual review control, it is often also critical to understand the source of the data being reviewed and analyzed. It is important to understand the flow of data reviewed in the report or summary and what criteria would create an outlier or exception that requires follow-up. It will also be important to document your review and, given it will be the first time through, consider erring on the side of caution and documenting more than may be needed. The reason for this is so you may clearly recreate the review and walk either internal or external auditors through your thought process and conclusions. Consider maintaining documentation in either a GRC solution already in use or on a shared drive or collaboration site.

Q. With our remote workforce, how do we confirm the tone at the top continues to promote a strong control environment amongst my team?

A. In our experience, in times of significant change, it is prudent for organizations to send refreshed messaging to emphasize the organization's existing standards of conduct and commitment to integrity and ethical values.

Without a strong tone at the top to support a strong culture of internal control, awareness of risks can be undermined, responses to risks may be inappropriate, control activities may be ill-defined or not followed, information and communication may falter, and feedback from monitoring activities may not be acted upon or heard.

Targeted messaging can be refreshed and communicated through entity-level control activities and programs that support tone at the top such as the following:

- Messaging from leadership through various methods of communication (for example, webcasts, newsletters, and emails)
- Annual code of conduct training and certifications
- Whistleblower hotline program
- SOX 302 certification program

In addition to internal messaging, consideration should be given to the inclusion of third parties, such as outsourced service providers, who provide services that affect an organization's system of internal control.

ICFR

Q. As a result of COVID-19, we will need to update the SOX risk assessment. What are the common areas affected?

A. Some common areas of the SOX risk assessment that may see an impact are:

- Transactions and accounting estimates affected by a decrease in revenue
- Supply chain issues
- Financial reporting activities affected by resource issues and availability and access to data
- Information technology risks that surface from a transition to a remote work environment
- Debt and financing transactions affected by changes in expected cash flow
- Impacts from third parties, such as customers, vendors, and outsourced service providers
- Considerations to determine if the affected area is material when considering quantitative and qualitative factors

Q. Should we expect SOX compliance to be loosened up due to COVID-19?

A. As of the time this is being written, other than the SEC order that gives public entities an additional 45 days from the original due date to file reports that would otherwise have been due from March 1 to July 1, 2020, there are no other changes to regulatory requirements associated with SOX if you meet specified conditions. PCAOB chairman William D. Duhnke III recently stated that "adherence to our standards takes on added importance as investors depend now, more than ever, on the integrity of financial statements."

Q. Are there any impacts of COVID-19 on entity-level controls that we should be thinking about?

A. Varying circumstances may affect entity-level controls for each issuer. Common circumstances and the related entity-level control activities affected may include:

- New or changes in risk factors that apply to financial statements, such as:
  - SOX risk assessment, which generally comprises activities identifying risks of material misstatements over the financial statement accounts and disclosures, including the consideration of IT risks and fraud risks, and activities to select or design controls to mitigate the risks
  - Policies and procedures related to control documentation
- Resource matters (such as availability of people or changes in roles and responsibilities) that might include:
  - Delegation of authority
  - Succession activities for onboarding control owners
  - Segregation of duties
  - 302 certification programs
  - Monitoring controls over third-party service providers

Q. We use several service organizations for key accounting transactions, what should we consider as it relates to their ability to reliably execute their processes and controls?

A. External organizations essential to the control environment may face a unique set of operational and internal controls challenges. Companies should consider maintaining consistent contact with outsourced service providers to evaluate their ability to continue to operate, including the evaluation of the extent to which additional oversight of the outsourced provider is required. Also consider assessing what temporary changes outsourced services providers have made to their control environments, as well as assessing the likelihood of receiving at a future point in time a service organization report (such as SOC-1) that is qualified. Other considerations include assessing whether alternative controls exist that are responsive to the outsource service providers deemed to be at most risk, and considering if the company should use an alternative service provider or whether critical outsourced functions could be brought in-house.

Q. Given the rapid change in business environment, should we consider the need for enhanced monitoring processes over daily/weekly transaction controls?

A. In our experience, primary drivers and initiators for enhanced monitoring are the processes, risks, and controls affected by COVID-19 as opposed to only control frequency. Enhanced monitoring activities may vary based on the change the impact has to the business environment and adapting to management's priorities.

Examples of primary activities management may perform to identify affected controls include:

- Update the risk assessment for COVID-19 considerations to identify impacted controls or the need for new controls to mitigate new or changing risks
- Leverage SOX 302 certification by designing specific questions to deploy to business process and control owners to identify impacted process and controls

Upon identification of impacted areas, organizations may determine that enhanced monitoring is necessary and update control activities to reflect the enhancement. A few examples that may require enhanced monitoring include:

Example type of impact	Examples of enhanced monitoring activities
Changes in people performing control activity	• Carry out onboarding activities effectively • Perform additional review during the transition period • 302 certification program to identify affected controls
Changes in how people are performing and evidencing the control	• 302 certification program to identify affected controls • Consider the need for additional levels of review, depending on the change • Consider the need for additional documentation (such as meeting minutes) and electronic sign-off and other evidence (such as a screenshot of meeting attendees)
Areas that are more susceptible to management bias for fraud, such as management estimates involving assumptions or critical judgments that will potentially be affected by COVID-19 issues (such as an update of revenue projections or supply chain disruptions)	• Perform additional reviews and/or enhance professional skepticism to challenge the appropriateness of assumptions and/or judgments • Dual authorization at varying levels of authority
Thresholds may be exceeded due to COVID-19 impacts, requiring investigation and response	• Perform additional reviews and/or enhance the professional skepticism applied to the review of threshold explanations and responses, as variances could be explained as COVID-19–related when they are not, which may mask an underlying issue
IT controls where IT resources are focused elsewhere due to needing to set up remote work	• 302 certification programs to identify affected controls • Increased frequency and/or precision of user access review where significant access changes occurred

Q. What is the potential impact of COVID-19 on control frequencies?

A. Resources may be constrained, which could potentially affect the performance of a control. In such cases, we have observed some issuers temporarily modifying control frequencies to a lesser frequency—for example, modifying monthly occurrence to quarterly or weekly to monthly. Before changing the control frequency, you may want to assess some design considerations, including:

- Will a change of control frequency to a lesser occurrence still serve to prevent or detect the material misstatement on a timely basis?
- Will the control performer be able to execute the control with the same level of precision?
- Will the reports or information used in the control need to be modified to align with frequency?

Ultimately, the decision should be risk-based, so changes should be documented and communicated to the parties affected, including parties such as:

- Those who perform the controls to reestablish baseline understanding of updated control frequency
- Those who test the controls (for example, external auditors and management's testers), as design conclusions will consider the new frequency
- Those who have oversight for internal controls (such as senior leadership and the audit committee)

Q. How can the SOX 302 certification program be leveraged as a monitoring control?

A. The SOX 302 certification program, including subcertifications, can be leveraged by designing specific questions to identify affected processes, risks, and controls. Upon identification, management should then consider assessing results to determine the appropriate response to mitigate risks.

The following are sample questions that could be deployed to business process and control owners, including those responsible for overseeing significant outsourced service providers:

- Have there been any significant changes to controls as a result of COVID-19, such as:
  - Control owner change
  - Change in control performance (such as change in timing of control performance, level of documentation, evidence of review, or steps or procedures performed)
  - Control not performed
- Have there been any significant changes to processes as a result of COVID-19, such as:
  - Process owner changes
  - Process performance changes (such as changes to the flow of transactions or alternate processes implemented as a workaround)
- Have there been any significant changes to or use of tools or technologies used in controls or processes not already contemplated above? For example:
  - Change in access to tools or technologies (e.g., you had to be granted access, or have a role change, to a tool or technology. If so, identify tool and/or technology)
  - Have you used any tools or technology differently since working remotely (for example, as a result of slow or unreliable Internet connections or VPN access difficulties)?
- For the outsourced service providers (OSP) you have responsibility for, has there been, or do you expect, disruption to the services provided?

Q. Are there any common fraud schemes that may percolate in this type of environment?

A. The impact of COVID-19 may result in an increase in incentives, pressure, and opportunities to perpetrate fraud. Issuers should consider updating the fraud risk assessment based on their specific facts and circumstances. The following are examples of areas that may have a higher susceptibility to fraud:

- Overstatement of revenue: Companies may endeavor to overstate revenue.
- Understatement of accounts receivable reserve: End customers may delay payments, and companies might not timely adjust for the high risk of nonpayment.
- Lack of inventory impairments: Disrupted supply chains and the inability to transport certain items due to import or export restrictions may offer companies an opportunity to reduce inventory write-offs this year. The valuation of the inventory may be called into question, and companies may attempt to overvalue the inventory for insurance purposes.
- Accounting estimates affected by revenue projections or supply chain issues: Inherent bias by management to either overstate or understate financials, given the pressures or motivation by management.
- Big bath charges: Given the financial loss associated with the consequences of the pandemic, companies may be motivated to write off underperforming assets that are either marginally associated with the pandemic impact or not associated at all.
- Capitalization of expenses: It is often tempting for companies to capitalize on expenses and deduct them over several accounting periods rather than expense the entire cost immediately.
- Health-related costs may be substantial, and executives may be inclined to spread the costs out over a few years rather than expense them when they occur.
- Disclosure fraud: Companies may be motivated to not fully disclose the impact of the pandemic to its overall business results, particularly as it relates to contingencies and misrepresentations surrounding the impact on the business.
- Business interruption insurance claims: Companies may be motivated to misstate the impact of the pandemic on its operations to generate additional insurance proceeds that warranted.

Q. How will I effectively perform my manual management review controls that rely on data from shared drives?

A. To the extent that you can access the data from a shared drive, continue to perform the management review control as designed. If you are not able to access the data on the shared drive, consider working with your management, and potentially IT, to identify a secure way of obtaining the information required to perform the control. Should a workaround be necessary due to working remotely, reference Question #4 about documenting changes to defined processes and controls.

Cyber

Q. As teams are moving to a remote work environment, is management providing increasing awareness of security leading practices in remote work, including elevated threats from phishing attacks?

A. As the organization moves to a remote work environment, now is the time to review and update policies, training procedures, and communications, especially those focusing on elevated threats and attacks. Examples of some activities management may want to consider performing as a result of the change to a remote work environment include:

- Identify areas that may require updated policies to accommodate changes to regular operating procedures.
- Communicate policies (and updates), expectations, and available resources to employees and contractors.
- Continually update cybersecurity awareness, education, and training to focus on current and pervasive phishing campaigns and social engineering attack vectors (COVID-19–related schemes).
- Provide clear guidance and procedures for suspected malware incidents, particularly ransomware, so employees may take immediate action and help contain incident damage and spread.

Q. Are we prepared for a remote working environment with updated identity management capabilities to enable seamless remote access management?

A. As many users must now access corporate systems and applications remotely, another focus area to consider is secure identity, as well as access management considerations. This includes understanding who is accessing systems, location specifics, and if they are authenticated and authorized. Consider reviewing user roles and permission sets to accommodate new work requirements (such as rotational roles or remote access permissions for rulesets that traditionally may not allow for remote access). Consider enforcing authentication for network and cloud-based systems and applications based on risk, including MFA and single sign-on (SSO). Also consider implementing privileged access management (PAM) for superuser access requirements. Finally, confirm the use of least- privilege principles across enterprise applications and systems.

Q. We might have to quickly stand up several cloud-based collaborative tools for accounting and internal controls documentation. What should we consider (for example, security and privacy) as we set up and leverage those tools for internal controls over financial reporting?

A. Collaboration technologies, while vital during the surge of virtual work, may pose threats to organizational security and privacy without proper management. This may also affect the internal controls over financial reporting. As these technologies expand their reach and prevalence in business operations, organizations should keep a pulse on potential threats, enact controls—where feasible—and promote service availability. Some areas to consider focusing on include identifying potential loopholes and security vulnerabilities associated with the use of collaboration technologies, implementation of risk-based platform controls to prevent inappropriate information access, and the development of role-based education and awareness guidelines around collaboration applications and remote work.

Q. Should cyber teams focus on the elevated landscape by enabling security monitoring, threat intelligence, and hunting?

A. As the situation evolves, examples of cyber practices to consider include developing a risk-based prioritized security strategy and strengthening of basic security coverage. This may include enhancing threat monitoring capabilities and hunting for threats within your network(s). Examples of actions organizations can take include re-baselining traffic patterns and tuning endpoints for new processes, expanding the scope of threat intelligence, confirming coverage for high-risk areas (such as data protection or insider threats), integrating data leak prevention (DLP) and document rights management into monitoring tools, and updating security incident response playbooks to reflect potential new threats or risks.

Q. What are some common cyber threats or phishing attempts that have arisen from this crisis?

A. Cyber threats have increased recently, many by leveraging the COVID-19 virus to exploit public panic. Since the severe outbreak began, cybersecurity analysts have identified many threats and phishing attempts targeting end users, home networks, and collaboration technology. Among them, spam and malware attacks are often sent with COVID-19 subject matter, links, and/or attachments. Educating employees about current threats, the dangers of opening attachments or clicking links from untrusted sources, and the actions needed to prevent virus infection are continued cyber hygiene and awareness recommendations.

Q. Are there data privacy or sensitive data risks we should be managing in our remote work environments?

A. As data, including personally identifiable information and other sensitive data (such as financial information) moves across remote work conditions, there may be an impact on data security. Below are some examples of steps an organization could consider taking related to managing data privacy or sensitive data risks:

- Identify deviations from normal data flows and the implications on laws and regulations. Consider whether explicit consent is required to adjust processes.
- Evaluate the implications of shifting privacy directives on business processes.
- Determine contractual coverage for third-party support areas.
- Review data protection strategies to accommodate operational shifts and implement privacy by design (PbD) where feasible. Disseminate notices to customers where applicable.
- Conduct a threat and risk assessment of new technologies, including integration with data privacy regulations.

Operations

Q. With my remote team and work environment, what are the critical things we should remember when performing our internal controls over financial reporting?

A. The objective should be to continue to perform the relevant controls that mitigate risks identified. To the extent possible, perform the same procedures and controls as if you were in the office. Should you need to develop a workaround outside of the defined processes and controls due to the remote work environment, then examples of considerations include:

- Clearly define and document the adjusted process and controls
- Identify changes to roles and responsibilities and maintain segregation of duties
- Ensure proper management approvals are received
- Communicate the modified process and controls to all relevant parties
- Maintain accurate documentation to evidence the controls performance, even though it may be different than evidence maintained in the past

As a reminder, performing a risk assessment is an iterative process and should be revisited periodically and more often as the circumstances warrant.

Q. Are remote meetings just as effective as in-person meetings? Is there an impact to internal controls over financial reporting?

A. Remote meetings can be just as effective as in-person meetings, but it depends on specific facts and circumstances and whether live vs. remote meetings would affect ICFR. A potential challenge is keeping participants on a virtual meeting fully engaged and participatory in order to not compromise the precision and effectiveness of the relevant review type controls as designed. The activity of conducting a virtual meeting alone should not have an impact on ICFR without other processes, risk, or control changes. During virtual meetings, controls can still be sufficient and effectively performed, and appropriate evidence can still be maintained.

Note that reliance on tools for communication likely wouldn't affect ICFR, but reliance on emerging technology that affects financial reporting or performance of the control may.

Q. What might my job and Controllership in general look like 12 months from now?

A. As virtual work environments become the norm over the next few months, there will likely be an increased reliance on automation and digital technologies. This may include automation around not only the control environment, but also processes within the ICFR scope. We anticipate an uptick in governance, the implementation of risk and controls (GRC) solutions to manage certifications, controls review, and control testing automation. Other digital solutions that business process owners may leverage, will can drive an increased reliance on automated controls to avoid manual, detective reviews.

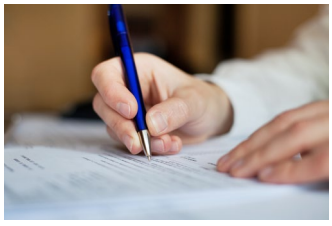
Q. How do I coordinate with my external auditor?

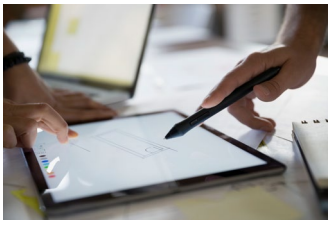
A. Most external auditors are familiar with performing work in a remote environment. It is recommended you maintain open communication with your auditor, which may result in more frequent, virtual communications, particularly related to any changes in processes and controls due to the current operating environment. A leading practice should be to have a standing touchpoint at least weekly to facilitate an open dialogue regarding the audit and/or project.

Q. A key control owner is not available 100 percent of the time, and we don't have a designee. How can we identify and document a designee?

A. Examples of activities an organization may consider performing if an employee is ill or no longer available full-time include:

- Assess which controls may be affected
- Determine if the identified control(s) requires a change to another compensating control or if assigning a backup with comparable skills and access rights may be effective
- When looking for an alternate control owner, keep in mind what inputs are needed to build the content for review (for example, system reports or access to shared drives may be the most beneficial in helping identify the right control owner)





Taxes

Q. In a remote work environment, what should we be thinking about when coordinating tax reporting with the evolving accounting and finance processes?

A. Coordination of tax reporting in the remote work environment highlights the importance of effective communication within the tax function and its stakeholders, as well as planning for different scenarios and process changes. Now may be a good time to revisit relevant accounting and finance processes and controls affecting the tax reporting process and gain an understanding of any modifications as a result of the current operating environment. For example, there may have been changes to a process that obtains critical financial data for purposes of preparing the income tax provision, or there may have been a change to a review or sign-off control, which may be relied upon by the tax department. Furthermore, access to essential accounting and finance personnel may be limited in the current operating environment, so you may need to plan well ahead of time, and to the extent necessary, a further process modification or contingency plan may be required. Similar to accounting and finance, tax personnel should consider developing workarounds outside of the defined processes and controls due to the remote work environment and consider how to best coordinate with other departments (such as accounting, finance, treasury, legal).

Q. As a result of COVID-19, we are revising our forecasts and projections of revenue and expenses. Are there additional income tax considerations that warrant attention?

A. The impact of COVID-19 may include significant adjustments to accounting estimates and forecasts, and management may be modeling various revenue and expense forecast scenarios based on numerous factors. When determining the impact of COVID-19 on income taxes, it is important to be consistent with models used for non-income tax purposes (such as impairment analysis) to those used for purposes of interim reporting of income taxes, valuation allowance considerations, and cash tax planning related to the CARES Act (incentives, credits, and potential carryback opportunities). It may also be important to have discussions with your external auditor early on in the process so they can weigh in on the potential impact on the accounting for income taxes, particularly in the current operating environment.

Q. With many jurisdictions changing tax deadlines, how do we track compliance and make sure we meet filings, elections, reporting, and disclosures?

A. As governments around the world are implementing various tax measures to stimulate their economies, the respective changes and new requirements may seem overwhelming. Depending on your circumstances, the existing processes to track compliance requirements may warrant the allocation of additional resources within an organization, further consideration to or greater use of tax technology tools, and/or assistance from your advisers. It may be time to revisit the effectiveness of tax controls relating to changes in tax laws and rates and consider whether there is increased risk due to the ever-changing tax environment. To mitigate any increased risks, tax controls may need to be modified to define additional owners and/or include additional data sources, checklists, or review procedures.

Contacts

Julie Velayo
Principal
Deloitte Risk & Financial Advisory
julievelayo@deloitte.com
+1 704 227 1425

Patty Salkin
Managing Director
Deloitte Risk & Financial Advisory
psalkin@deloitte.com
+1 609 806 7279

Lindsay Rosenfeld
Managing Director
Audit &Assurance
linrosenfeld@deloitte.com
+1 313 396 3167

Neil White
Principal
Deloitte Risk & Financial Advisory
nwhite@deloitte.com
+1 212 436 5822

Mike Kosonog
Partner
Deloitte Risk & Financial Advisory
mkosonog@deloitte.com
+1 313 396 3622

Samantha Pietsch
Managing Director
Deloitte Tax
spietsch@deloitte.com
+1 213 996 4304

Joe Sutter
Manager
Deloitte Risk & Financial Advisory
jsutter@deloitte.com
+1 571 429 1446