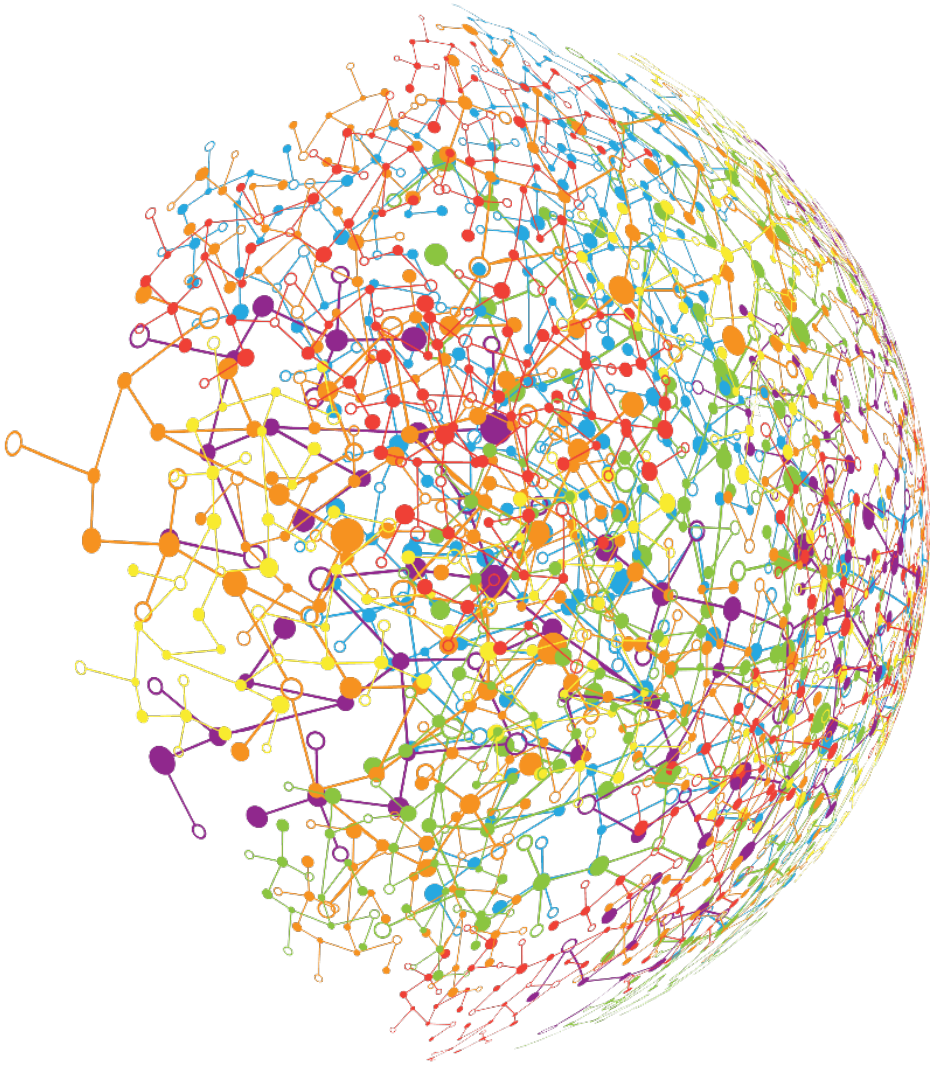
Deloitte.



Reacting to COVID-19 in Internal Control over Financial Reporting

March 2020

Helping organizations anticipate challenges in internal control over financial reporting

As organizations around the world rapidly enact their crisis recovery plans and focus on ensuring the safety of their people and their assets, business as usual activities risk being interrupted or cancelled. Financial reporting processes are no exception; however, at a time of such exceptional uncertainty there continues to be a need to give investors, regulators and other stakeholders relevant and timely information about operational and financial performance.

The Securities and Exchange Commission (SEC) has issued guidance to companies regarding relief related to delayed filings; however, at this time it is difficult to predict if any further financial reporting requirements may be eased if the impact of COVID-19 extends for many months and what dispensations may be given in such a future scenario.

"Actual effects will depend on many factors beyond the control and knowledge of issuers. However, how issuers plan for that uncertainty and how they choose to respond to events as they unfold can nevertheless be material to an investment decision."

Jay Clayton, SEC Chairman

The situation is likely to evolve rapidly, and further clarity may be provided in due course. However, with a number of organizations having March and April year-ends or interim financial reporting requirements in this period, we have identified certain internal control over financial reporting matters that, at this time, are potential challenges for management as a result of the impacts of COVID-19.

At this stage, our considerations focus on maintaining the existing control environment and include the following:

1. **Reassessing the financial reporting timeline** and relaxing timing constraints, where possible, on the operation of key controls. This will likely need to be part of management's risk assessment to ensure that all key controls operate in the appropriate time period (e.g., prior to year-end, for many controls), but potentially some controls may need to operate simultaneously rather than in the traditional step-by-step hierarchy of the financial reporting process.
2. **Formally documenting where certain decisions have been made** to provide temporary relief, for example changes in timelines or new responsibilities being granted, so that it can be evidenced to auditors, including financial statement and service auditors, at a later date (via email or other means).
3. Keeping in mind that **fraud risks may change** in such a time of crisis, as new opportunities are enabled for both internal and external parties. Incentives for committing fraud — both misappropriation of assets and financial reporting fraud — may also be heightened, especially if significant redundancies are likely to be required or employees suffer significant personal financial stress. However, for some organizations, misappropriation of physical assets may, become less likely with more employees working remotely.
4. Ensuring early and on-going **discussion with auditors, including financial statement and service auditors,** to avoid surprises later in the year. Audit approaches are likely going to need to evolve as well.

The extent to which an organization will ultimately be impacted is difficult to predict at this relatively early stage of the COVID-19 outbreak. We anticipate that organizations with increased automation and who have significant amounts of technology in their control environment will have different challenges to address as compared to those with a more manual control environment. However, neither approach is free from potential pitfalls that may occur in the coming weeks and months.

Changes to the control environment are likely to be needed and, based on the current situation, impacts may be felt in the following key areas:

1. **Scoping and risk assessment conclusions** may need to be revisited to verify that they are appropriately responsive to the changes in the organization that have occurred since the outbreak of COVID-19, such as:
    - Revenue, supply chain, technology and other infrastructure disruption.
    - Processes that are reliant on select few resources (e.g., highly technical areas, estimates, and significant judgments) and may require updates to delegation of authority.
    - Processes that are highly manual.
    - Areas that are susceptible to fraud (e.g., money movement).
2. **The design of controls** may need to be adjusted (as well as appropriate documentation of the adjustment maintained) to compensate for changes in risk, or contingency plans may need to be put in place for outsourced service providers.
3. Evaluation of the operating effectiveness of controls may need to include a **plan for increased levels of remote testing**. This will likely also result in an increased focus on the quality of documented evidence to support the evaluation of the operating effectiveness of controls, in particular a management review control where judgment is used by testers to evaluate the sufficiency ofthe documentation to support a conclusion that the control is operating effectively.
4. If an **increased level of deficiencies is identified as a** result of COVID-19, management will need to put in place plans for a timely and effective response. This will require careful project management and put increased pressure on those individuals with the best knowledge of internal control.
5. Typical **communication plans with senior management and board members** may need to be revisited so that they are given the information they need on a timely basis to fulfil their responsibilities.

To respond to the matters above, extensive prioritization is needed, and it may be appropriate to put existing control transformation plans on hold. Project management will be key, especially if there are other significant business needs that have taken priority for some of the critical resources or management focus. Any existing remediation projects will likely have to be reassessed and expectations discussed early with the auditors, including financial statement and service auditors.

We outline below some potential considerations and responses that organizations may want to consider, focused around these different areas. This is not intended to be a comprehensive list and will vary depending on the facts and circumstances of each organization. Performing a tailored risk assessment, including going through each of the principles and points of focus in the COSO 2013 framework, will likely need to be performed as a completeness check.

Our separate analysis covering cybersecurity and general accounting and financial reporting requirements is also available. These may be updated frequently so please check the webpages listed below to get the latest updates.

- Deloitte's COVID-19 Web page.
- Deloitte's Cyber Web page.
- Heads Up newsletters.
- Financial Reporting Alerts on SEC reporting topics on DART (subscribers only).

Business control implications

Area	Considerations	Responses
Management review controls	Breakdown in review-type controls or the inability of individuals to perform control duties *(e.g., due to employee illness or the closure of affected offices).* Lack of reliable information may affect management's ability to effectively operate controls *(e.g., personnel may not be available in offices in affected areas to provide information that is essential to the effective operation of an internal control).* Inability for personnel to meet live and conduct meetings may impact the design or operation of the control.	Verify that control processes and narratives are up to date in the event control owners need to change. Establish that any new or temporary control owners have the appropriate authority and competency to perform the control activities (consider appropriate segregation of duties). Identify other controls that can provide the same assurance but use different information sources. Plan to implement new controls that provide additional assurance over the reliability of information *(e.g., manual checking back to source documents, such as invoices).* Enhance existing meeting controls to take into account reviews occurring remotely, including alternative means for holding meetings and a process to resolve questions raised during reviews. Evaluate whether changes to the criteria for investigation or the process for follow-up are necessary. Evaluate whether expectations used in controls that rely on the comparison of current financial information to the budget, forecast, or prior-period results remain appropriate.
Management review controls over complex accounting estimates *(e.g., impairment of goodwill and other intangible assets, fair value of financial and nonfinancial assets).*	Failure to consider the impact of new uncertainties and market volatility on significant accounting estimates.	Perform a top-down risk assessment of significant accounting estimates to identify where existing controls may need to specifically consider COVID-19 impacts and communicate the results of this to control owners. Verify that the disclosures to financial statements appropriately disclose the sensitivity of those key assumptions.

Area	Considerations	Responses
		Enhance existing controls to enable appropriate, and documented, consideration of COVID-19.
Equity method investments and joint ventures	Lack of access to timely or reliable financial information from an equity method investment or joint ventures.	Establish regular communication with management of the equity method investment or joint venture to monitor likelihood of impacts to the entity in upcoming financial reporting periods. Reconsider the materiality of each equity method investment or joint venture to the consolidated financial statements, to evaluate the in-scope key controls.
Transaction processing controls	Transactions may not be processed on a timely basis due to COVID-19 and as a result backlogs in transaction processing may form (on-shore or off-shore).	Have enhanced monitoring processes and controls to monitor the effectiveness of daily/weekly transaction processing controls. See additional considerations in the Risk assessment section below.
Cash payments controls	Payments may require a dedicated computer terminal or hardware for the validation of payments. Lack of availability to reach individuals to verify transactions / approvals. Backup contact details with the bank to verify potentially fraudulent payments are not updated. Insufficient dual payment signatories are available to approve payments. Changes in reporting / approval lines may not have been communicated to, or acted on, by the bank.	Test all processes involving online banking access to determine if they can be operated remotely. Review payment approvers listing, and risk assess whether expanding it is appropriate (being careful of segregation of duties). Ask bank for additional hardware devices and/or to relax hardware payment controls. Speak with bank to discuss emergency contact details and failsafe processes.
Automated controls	If manually triggered and/or monitored, the automated control may fail to operate due to personnel being unavailable. Failures for other reasons may not be detected on a timely basis if monitoring of controls is not operating.	Identify which automated controls are most susceptible to failure, due to COVID-19, or based on historical trends. Verify that appropriate compensating or mitigating controls exist and are operating effectively to mitigate any risks arising from a failure to operate the automated controls.

Area	Considerations	Responses
Outsource service providers	External organizations essential to the control environment may face their own challenges, which could impact on their ability to reliably execute their processes and controls upon which reliance is placed.	Contact outsourced service providers to evaluate their ability to continue to operate in accordance with established service level agreements (SLAs) or key performance indicators (KPIs), including monitoring of their service providers. Assess the likelihood of receiving at a future point in time a service organization report (*e.g., SOC-1*) that is qualified. Assess what temporary changes outsourced services providers have made to their control environments. Evaluate the extent to which additional oversight of the outsourced service provider is required. Assess compensating controls the outsource service providers deemed to be at most risk, and implement new or updated complementary user entity controls if required. Verify that contingency planning is in place in case an alternative service provider needs to be used. Consider changes to conclusions on what activities need to be outsourced, versus what is currently outsourced based upon changes to your risk assessment.
Insider trader concerns	Employees may have access to nonpublic information, and trading restrictions may need to be imposed, as the potential effects of COVID-19 could constitute material nonpublic information. This risk may be elevated if the financial reporting timeline is extended.	Entities should consider how their codes of ethics and insider trading policies address, prevent, and deter trading that is based on material nonpublic information, including information related to COVID-19. Communications to employees may be needed to remind them of their obligations.
Changes in current internal control projects	Likely to be similar to the potential considerations outlined below under IT control implications.	Likely to be similar to the possible responses outlined below under IT control implications.

IT control implications

Area	Considerations	Responses
Super User access	Organizations may have contingency or succession plans for senior executives; however, this may not adequately cover IT personnel. With increased dependency on IT personnel and infrastructure to support the organization working remotely, the availability or ability of IT personnel for internal control related matters could be limited. Key IT staff with administrative privileges may be unable to perform their duties (*e.g., due to illness*) and this may impact the ability of the organization to address IT failures, or operate key IT controls.	Assess the exposure of current IT capabilities, including outsourced activities, to determine where risk could be present. Consider cross training of IT staff to support multiple IT activities, subject to segregation of duties considerations. Consider using password vaults or other methods to enable administrative accounts to be used in a secure manner if a key individual is not available. Perform a pre-emptive review of IT controls to identify which users and super-users are most critical. Consider designing contingency plans for IT personnel, so that key controls can continue to be operated (segregation of duties should be considered as part of this scenario planning).
Outsource service providers	Likely to be similar to the potential considerations outlined above under business control implications.	Likely to be similar to the possible responses outlined above under business control implications.
Change management	Individuals try to shortcut the change management process because they believe COVID-19 will result in delays. Business personnel are unavailable to approve changes. Responsibilities change due to personnel being unavailable, and this may result in developers having access to promote changes to a live environment. With COVID-19 taking a significant amount of the organization's focus, inadequate testing of changes may be done before they	Communicate with the business to reduce the volume of changes requested, to critical items only. Verify that monitoring controls over change management continue to operate effectively during the period, to detect any deviations from required testing and approval processes.

Area	Considerations	Responses
	are allowed to go live. Critical changes may need to be made, but the relevant process could be dependent on personnel that may not be available or temporary personnel who are not adequately trained, leading to an error. Routine changes, such as application of security patches, not being completed timely due to more urgent priorities.	Verify that changes to developer access rights continue to be reviewed and perform mitigating procedures on a timely basis if issues are identified. Carefully review existing processes for addressing critical changes to verify that they remain pertinent and that only appropriate personnel are given these responsibilities. Independently challenge requests marked by the business as being critical to ascertain if this really is the case or if normal change processes should be followed.
Changes in current internal control projects	New systems or upgrades of systems may be delayed due to COVID-19, but there may be a significant need for this to be completed on schedule from an internal control over financial reporting perspective (*e.g., remediation of a significant deficiency or material weakness*). Key resources may be redeployed, resulting in the project being inadequately staffed or having inadequate expertise to execute successfully. A dependency on third-party vendors or external service partners for the successfully delivery of the project may exist, and these third parties could be unable to fulfil their requirements due to COVID-19.	Critically consider which projects need to continue and which can be put on hold for the short-term. Perform an up-front reassessment of timeline for key projects, to identify revised completion dates and to commence planning for any adverse consequences due to anticipated late delivery. Assess resource redeployments from key projects to determine the impact on the project timetable or to determine if additional activities, such as quality assurance, need to be performed so that project is completed successfully. Verify that contingency planning is in place in case an alternative service provider needs to be used.
Interface and batch processing controls	Monitoring of automated interfaces by relevant IT personnel may not occur on a timely basis or may fail to be performed.	Establish clear understanding of which interfaces are most critical and identify which have any form of manual

Area	Considerations	Responses
	Manual interfaces may not be operated if IT personnel cannot access the system remotely or are unavailable to do so.	dependency to operate. Consider designing contingency plans for IT personnel, so that key controls can continue to be operated (segregation of duties should be considered as part of this scenario planning). Identify whether monitoring activities can be spread across a wider population of IT personnel to mitigate risk on a single user or team.
Resilience and remote working	Lack of proper infrastructure to support remote working could impact the ability of people to log-on to applications and services. Remote working facilities may be overwhelmed or operate intermittently. Employees may seek to work-around existing security protocols and controls to keep the business operating efficiently, which could impact the confidentiality of information and result in the leakage of secure data. Reduction in force issues with IT support if companies have to reduce workforce due to profitability / going concern issues. Increase in hacker activity to try to exploit the crisis.	Prepare plans for the operation of essential IT controls outside of peak working hours (such as using offshore locations). Establish that appropriate security technologies, such as VPNs, support all critical applications and services, including, at a minimum, those that impact financial reporting. Communicate with employees to remind them of the existence of training materials, where they can go for support and not to circumvent security protocols. Establish correct and complete security configuration for any new hardware or software installed to support increase in remote access. Enhance monitoring of corporate network due to remote user's insecure home networks.

Internal control framework and governance

Area	Considerations	Responses
Scoping	Anticipated business performance measures used to scope the business may end up being significantly different from actual business performance measures resulting in last-minute changes to the scope.	Perform up-front scenario analysis on the SOX scoping to identify the likelihood of out-of-scope location, business units, or company codes being brought into scope. Prepare a short-list of areas that are most at risk and hold contingency planning meetings with those areas to determine their SOX-readiness capability.
Risk assessment	Organizations may fail to revisit risk assessment, inclusive of fraud risks, and instead rely on risk assessments performed prior to the COVID-19 outbreak. These may therefore fail to take into account: • Material changes to the financial reporting process or changes in the business. • One or more new risks that are qualitatively significant (*e.g., risk of a material volume of credit notes being issued*). • Pre-existing risks that may be heightened as a result of COVID-19 impacts (*e.g., inventory obsolescence, credit risk of customers*). Organizations may fail to continue ongoing monitoring to identify emerging risks and, as they present themselves, incorporate into risk assessment process.	Perform a top-down risk assessment to identify what may change or has already changed. Evaluate impacted areas for changes to people, process, and technology and update controls accordingly. Seek bottom-up feedback from the business to challenge the reassessment of risk. Document the revised risk assessment and conclusions reached as to where changes in processes and controls will be needed. Create or enhance existing policies and procedures to adapt to COVID-19 impact, inclusive of roles and responsibilities, timelines, and form of relevant artifacts. Communicate the results of any changes to process and control owners. Encourage control owners to raise their hands and ask for help if they encounter challenges in performing their controls. Consider the impact of COVID-19 on entity level controls. Engage with auditors, including financial statement and service

Area	Considerations	Responses
		auditors, to understand expectations. Raise significant changes to risks and control environment to boards.
Monitoring	Existing monitoring activities may fail to cover any newly implemented controls. Potential inability to access sites to perform observations, will impact management's ability to execute controls. Potential distractions resulting from being focused on COVID-19 response and may not execute normal monitoring of controls oversight.	Consider monitoring activities as part of the design of any new control activities. Leverage certification processes (*e.g., 302 subcertifications*) to gain insights on potential control frailties, people changes and processes impacted in order to risk assess and respond. Consider whether changes in monitoring controls, such as site visits by Internal Audit, are necessary, and how evidence will be obtained supporting management's assessment of ICFR.
Deficiency evaluation and concluding activities	Insufficient personnel, with adequate knowledge and experience, available to evaluate an increased number of deficiencies. Deficiencies reported later in the year due to challenges with performing audit activities, resulting in less time for management to mitigate or remediate the issues found.	Review the depth and capability of individuals with internal control responsibilities. Establish a "quick response" group that is tasked with evaluating deficiencies and making decisions on the best way forwards. Consider bringing in short-term project management expertise from elsewhere in the organization to establish good project management practices and to allow those individuals with internal control experience to focus on identifying and implementing solutions.
Communications	Failing to prepare for increased frequency and depth of communications to senior management and board members.	Establish accountable owners to summarize overall status and key issues being dealt with, typically one individual for business controls and another individual for IT controls.

Testing activities

Area	Considerations	Responses
Personnel Considerations	Organizations may have contingency or succession plans for senior executives, but there might not be contingency plans for internal audit personnel or designated back-ups for control performers. Personnel that are key to certain operations of the business may be from external organizations and may not be available (this could include both personnel that support management's assessment of ICFR or as part of the Internal Audit function). Process or control owners in the organization may not be available during the planned testing period.	Perform an up-front review of testing plans, and identify ways in which increased flexibility in testing schedules can be obtained. Seek alternative sources for testing individuals; this may require delaying activities that are deemed to be less critical. Seek ways to align the different testing groups such that the testing impact on the business personnel is minimized. Identify and prepare backup personnel (potentially secondary) for key responsibilities, including executing control activities. Confirm that essential positions have current procedural documentation that is suitable for a backup resource. Consider opportunities for labor arbitrage across geographies to build resilience.
Testing logistics	Measures put in place may mean that typical testing approaches are not feasible and remote testing may need to be performed in the majority of cases. This is likely to prove most challenging in areas such as: • Performing walkthroughs of the end to end process. • Performing operating effectiveness testing for management review controls or controls where evidence that has historically been centralized is now decentralized.	Establish regular communication between all testing parties (testers and those being tested). Agree which technologies will be used to support the testing, in particular communication tools and file-sharing platforms, and verify that all testing and business personnel can access these. Communicate with control owners to emphasize the importance of retaining

Area	Considerations	Responses
		high-quality evidence about the operating effectiveness of controls to support management's assessment. Prepare a contingency plan in case increased testing is necessary for the remediation of deficient controls.

About Deloitte