

## Internal controls

### Considerations related to COVID-19

High quality corporate reporting that includes disclosures of timely, reliable, insightful information is critical in the current environment. Auditors act as *part of a financial reporting ecosystem* that includes management, those charged with governance (TCWG e.g. boards, audit committees), regulators, standard setters, investors and other stakeholders. The purpose of the financial reporting ecosystem is to produce corporate reporting that is complete, accurate, and transparent. The foundation for the financial information is a sound internal control environment maintained by management and overseen by TCWG. One of the roles of the auditor is to understand an audited company's internal controls as part of determining the nature and extent of procedures to perform in order to evaluate whether the company's financial statements are fairly presented.

#### Considerations for companies

A company's management and TCWG should consider the broad implications of COVID-19 on the company's internal control environment, including management's ability to complete its financial reporting process and prepare financial statements on a timely basis. The Appendix below includes examples of impacted areas and key questions for companies to consider.

In addition to the increased complexities created by the current environment on developing estimates and making going concern judgments, there may be increased pressures and opportunities to commit fraud. While the risk of fraud is typically not a new risk, COVID-19 has caused significant operational and



financial disruption, resulting in increased pressures on businesses, their employees and their stakeholders. Weakened internal control environments where key control owners are working remotely or have been fired or furloughed, combined with situations where companies, their supply chain and customers may be distressed and struggling financially create opportunities for fraud – whether that is through manipulation of financial results, misrepresentation of facts or misappropriation of assets.

In accordance with most accounting and auditing frameworks, the primary responsibility for the prevention and detection of fraud rests with both management and TCWG<sup>1</sup> of the company. Companies typically have a process in place, monitored by TCWG, to identify and assess risks and ensure there are controls in place that prevent and detect misstatements. Management and TCWG should assess the heightened risk of fraud presented by the COVID-19 environment and ensure their control environment is able to mitigate such risks, including re-evaluating their fraud risk assessments in response to the current environment and throughout the year as circumstances change.

## Considerations for auditors

Auditors recognize that evaluating internal controls has never been more important, and it should not be treated as a discrete part of the audit. There are likely to be changes to certain controls that have been operating throughout that 12-month period. For example, these changes could include changes in control operators due to staffing changes, changes in documentation of control operation due to remote workforce, or changes in control frequency/consistency due to competing priorities. These changes could apply to the entity or outsourced service providers used by the entity. Auditors should consider the potential for changes in evaluation of the design of controls and tests of operating effectiveness throughout the period of the audit. Auditors are also responsible for assessing the risk of material misstatement due to fraud.

Deloitte is responding to challenges presented by COVID-19 using a coordinated approach. At Deloitte, we take our responsibilities in serving the capital markets and the public interest very seriously and we are deeply committed to investing in capabilities and continuous improvement to deliver high-quality audit services.

## Connect

If you would like to discuss Deloitte Global initiatives further, please reach out to **Alex Schillaci**, Managing Director – Global Regulatory, [aschillaci@deloitte.com](mailto:aschillaci@deloitte.com) or **Dave Sullivan**, Managing Director – Global Audit & Assurance Quality, [dsullivan@deloitte.com](mailto:dsullivan@deloitte.com).

Deloitte Global A&A has taken several actions to support engagement teams in evaluating and testing internal controls in the COVID-19 environment, including the following:

1. Internal controls and fraud risks as a featured topic on the weekly COVID-19 webcasts for Audit Quality, Regulatory, and Risk Leaders webcast.
2. In March-April 2020, issued on-going, clear, and consistent guidance and toolkits for Deloitte practitioners and audited companies such as (not all inclusive):
  - a. *Internal Control Considerations in a COVID 19 Environment* containing practical guidance and tips.
  - b. *Forensic Focus on COVID-19: Financial Statement Fraud*, highlighting areas that may be more susceptible to fraud created by adverse events such as COVID-19.
  - c. *Reacting to COVID-19 in Internal Control over Financial Reporting paper* to help organizations anticipate challenges in internal control over financial reporting, including business and IT control implications, internal control framework and governance, and control testing considerations.
3. Additional activities are put in place to remind practitioners of their professional obligations, importance of the increased level of the professional skepticism, including frequent leadership messaging and strong tone at the top that “we are not done until we are done,” and presentations by the Global Ethics Leader.

<b>Pressure</b>	Management should be vigilant of the pressure to perpetrate fraud created by the distress of COVID-19 including: <ul style="list-style-type: none"> <li>• Pressure to keep the company a going concern</li> <li>• Pressure to inflate share prices or pay dividends and thus maintain distributable reserves</li> <li>• Pressure to continue to pay employees and suppliers</li> <li>• Pressure to meet bank and other covenants</li> <li>• Financial pressures on individual employees due to lost jobs, pay-freezes/cuts, unpaid leave, no bonuses or promotions</li> <li>• Pressure to report all bad news now and make un-necessary write-offs that can be wrongly attributed to COVID-19</li> </ul>
<b>Rationalization</b>	There will be those that see this as an opportunity to commit a fraud believing they are less likely to get caught as the current disruption draws management’s attention to other areas. In addition, those that would not normally commit fraud may see it as acceptable in these circumstances ‘for the greater good’ of protecting their company, employees, or themselves.
<b>Opportunity</b>	Disruption and changing working patterns may lead to companies needing to change their usual internal controls to allow operations to continue. For example: approvers of journal entries or other financial decisions may change if key people are off work; system access rights for employees may be increased to allow remote working; and documentation requirements may be reduced. However, disruption may cause existing fraud schemes to surface as the perpetrators are unable to keep them hidden.

<sup>1</sup> <https://www.aicpa.org/content/dam/aicpa/eaq/audit-committee-checklist-coronavirus-covid-19.pdf> represents a list of questions that those charged with governance should consider asking companies’ management.

## Appendix






### COVID-19: Control environment considerations

Due to the “black swan” nature of this pandemic, there is limited precedent as to how COVID-19 will impact organizations’ control environments. Many companies are experiencing discrete financial “shocks” and broader day-to-day disruption that are directly challenging their risk, control, and defense models. Below are examples of impacted areas, key questions, and considerations based on early client discussions:

	Risk assessment impact	Effective allocation of resources	Key service organizations reliance	Remote access	Execution of controls and monitoring	COSO internal control framework components
Key questions	What is the effect of COVID-19 on the organization’s current risk assessment and risk landscape?	Are resources allocated to the appropriate activities based on current environment? Are sufficient training and onboarding documents provided for individuals to serve as backups?	What is the extent of business disruption for key service providers? Do additional oversight procedures need to be established during this period of disruption?	Have users been appropriately provisioned remote access for their job functions? Have you established mechanisms to continue to monitor the remote control environment?	Are individuals aware of what is mission critical? Have decisions been made about required control modifications? Have you considered the need for enhanced monitoring processes over daily/weekly transaction controls?	<ul style="list-style-type: none"> <li>Control environment</li> <li>Risk assessment</li> <li>Control activities</li> <li>Information and communication</li> <li>Monitoring</li> </ul>
Considerations	<ul style="list-style-type: none"> <li>Revisit risk assessments, inclusive of fraud risks, and adjust for potential COVID-19 impact, for example:                             <ul style="list-style-type: none"> <li>Revenue, supply chain, technology, and other infrastructure disruption</li> <li>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</li> <li>Processes that are highly manual</li> <li>Areas that are susceptible to fraud (e.g., money movement, insider trading, theft of physical assets)</li> </ul> </li> <li>Monitor for emerging risks, and as they present themselves incorporate into risk assessment process</li> </ul>	<ul style="list-style-type: none"> <li>Identify and prepare back-up personnel (potentially secondary) for specific responsibilities, including executing control activities</li> <li>Review segregation of duties to ensure continued enforcement</li> <li>Confirm that essential positions have current procedural documentation that is suitable for a backup resource</li> <li>Consider opportunities for labor arbitrage across geographies to build resilience</li> </ul>	<ul style="list-style-type: none"> <li>Contact outsourced service providers to evaluate their ability to continue to operate in accordance with established SLAs / KPIs, including monitoring of their service providers</li> <li>Assess what temporary changes outsourced services providers have made to their control environments</li> <li>Evaluate the extent to which additional oversight is required</li> <li>Consider changes needed to what is currently in- vs. out-sourced based upon changes to your risk assessment</li> </ul>	<ul style="list-style-type: none"> <li>Scrutinize user access to assess only required access has been granted</li> <li>Consider using password vaults or other methods to ensure administrative accounts can be used in a secure manner if a key individual is not available</li> <li>Pre-emptively review power- and super users for restrictions and adequate backups</li> <li>Communicate with the business in order to reduce the volume of system changes requested to critical items only</li> <li>Enhance monitoring of corporate network due to remote users insecure home networks</li> <li>Leverage certification processes (e.g., 302 sub-certifications) to gain insights on potential control frailties, people changes, and impacted processes in order to risk assess and respond</li> </ul>	<ul style="list-style-type: none"> <li>Focus on how reviewers are evidencing review and approval through electronic means (e.g., emails, e-signatures)</li> <li>Identify which automated controls are most susceptible to failure, due to COVID-19, or based on historical trends</li> <li>Consider alternatives for controls that require physical observation (e.g., use of drones to conduct physical inventories by independent personnel)</li> <li>Ensure appropriate monitoring controls exist and are operating effectively to mitigate any risks arising from a failure to operate the automated business controls</li> </ul>	
Linkage to COSO <sup>1</sup> components   More can apply, based on our assessment						

<sup>1</sup> Committee of Sponsoring Organizations of the Treadway Commission (“COSO”) Internal Control Framework Components

# COVID-19: Control environment responses

 Communication considerations	 Preparation for future controls assessments	 Additional resources
Have you considered the need for enhanced communications to both internal and external parties?	Have you considered updating your control descriptions or creating alternative controls?	For updates on COVID, information on new guidance, and resources available to you, please visit:
<ul style="list-style-type: none"> <li>• Consider reinforcing the importance of control execution (e.g., newsletters, videoconference)</li> <li>• Encourage control owners to raise their hands and ask for help if they encounter challenges in performing their controls</li> <li>• Communicate with control owners to emphasize the importance of retaining high-quality documented evidence to support testing programs</li> <li>• Promote open and on-going communication with key service providers in order to identify the need to alter the current interaction model</li> <li>• Establish accountability and owners for communicating key issues being dealt with and to provide on-going status</li> <li>• Consider the latest SEC disclosure guidance on reporting the effects and risks of COVID-19 on your business, financial condition, and results of operations</li> </ul>	<ul style="list-style-type: none"> <li>• Create or enhance existing policies and procedures to adapt to COVID-19 impact, inclusive of roles and responsibilities, timelines, and form of relevant artifacts</li> <li>• Evaluate impacted areas for changes to people, process, and technology, and update controls accordingly</li> <li>• Engage with all testing parties (testers and those being tested), including financial statement and service auditors, to understand/communicate expectations</li> <li>• Raise significant changes to risks and control environment to senior management and boards</li> <li>• Prepare for the likelihood of remote testing and the need for greater cooperation with both internal and external parties involved in testing</li> <li>• Consider the use of technologies to support the testing, in particular communication tools and file sharing platforms, to allow testers and business personnel to assess required information</li> <li>• Prepare a contingency plan in case there are increased levels of findings</li> </ul>	<ul style="list-style-type: none"> <li>• Deloitte COVID-19 homepage: <a href="http://www.deloitte.com/covid-19">www.deloitte.com/covid-19</a></li> <li>• "IFRS in Focus" newsletters: <a href="http://www.iasplus.com">www.iasplus.com</a></li> <li>• "Heads Up" newsletters: <a href="http://www.deloitte.com/us/audit">www.deloitte.com/us/audit</a></li> <li>• Financial Reporting Alerts on SEC reporting: <a href="http://www.dart.deloitte.com">www.dart.deloitte.com</a> (subscribers only)</li> <li>• SEC COVID-19 response section: <a href="https://www.sec.gov/sec-coronavirus-covid-19-response">https://www.sec.gov/sec-coronavirus-covid-19-response</a></li> <li>• SEC press releases: <a href="https://www.sec.gov/news/pressreleases">https://www.sec.gov/news/pressreleases</a></li> <li>• Mitigate efforts through controls modernization: <a href="https://www2.deloitte.com/us/en/pages/financial-advisory/articles/controls-testing-and-compliance.html">https://www2.deloitte.com/us/en/pages/financial-advisory/articles/controls-testing-and-compliance.html</a></li> </ul>

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other.

DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

This document contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this document, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this document. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2020. For information, contact Deloitte Touche Tohmatsu Limited.