Deloitte.

# COVID-19: Control environment considerations

There is limited precedent as to how COVID-19 will affect organisations' control environments. Many organisations are experiencing discrete financial "shocks" and broader day-to-day disruptions that are directly challenging their risk, control, and defense models. Below are examples of affected areas, key questions, and considerations based on early client discussions.

| | Risk assessment impact | Effective allocation of resources | Key service organisations reliance | Remote access | Execution of controls and monitoring |
|---|---|---|---|---|---|
| Key questions | **What is the effect of COVID-19 on the organisation's current risk assessment and risk landscape?** | **Are resources allocated to the appropriate activities based on the 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 monitoring 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?** |
| Considerations | • Revisit risk assessments, inclusive of fraud risks, and adjust for the potential COVID-19 impact. For example:<br>– Revenue, supply chain, technology, and other infrastructure disruption<br>– Processes requiring select few resources (e.g., highly technical areas, estimates, and significant judgements); these may require<br>– updates to delegation of authority<br>– Highly manual processes<br>– Areas that are susceptible to fraud (e.g., money movement, insider trading, and theft of physical assets)<br>• Monitor emerging risks, and as they present themselves incorporate them into the risk assessment process. | • Identify and prepare a backup team (potentially secondary) for specific responsibilities, including executing control activities.<br>• Review segregation of duties to ensure continued enforcement.<br>• Confirm that essential positions have the current procedural documentation that is suitable for a backup resource.<br>• Consider opportunities for labour arbitrage across geographies to build resilience. | • Contact outsourced service providers to evaluate their ability to continue to operate in line with established SLAs/ KPIs, including monitoring of their service providers.<br>• Assess what temporary changes outsourced services providers have made to their control environments.<br>• Evaluate the extent to which additional oversight is required.<br>• Consider changes needed to what is currently in- vs. out-sourced based upon changes to your risk assessment. | • Scrutinise user access to assess that only required access has been granted.<br>• Consider using password vaults or other methods to ensure the use of administrative accounts in a secure manner if a key individual is not available.<br>• Pre-emptively review power and super users for restrictions and adequate backups.<br>• Communicate with the business to reduce the volume of system changes requested to critical items only.<br>• Enhance the corporate network monitoring as remote workers use insecure home networks.<br>• Use certification processes (e.g., 302 sub-certifications) to gain insights into potential control frailties, people changes, and affected processes to assess risk and respond. | • Focus on how reviewers are evidencing review and approval through electronic means (e.g., emails and e-signatures).<br>• Identify which automated controls are most susceptible to failure (due to COVID-19), or based on historical trends.<br>• Consider alternatives for controls that require physical observation (e.g., use of drones to conduct physical inventories by independent workers).<br>• Ensure appropriate monitoring controls exist and are operating effectively to mitigate any risks arising from a failure to operate automated business controls. |
| Linkage to COSO[1] components \| More can apply, based on our assessment | | | | | |

COSO internal control framework components

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

# COVID-19: Control environment responses

## Communication considerations

Have you considered the need for enhanced communications to both internal and external parties?

- Consider reinforcing the importance of control execution (e.g., newsletters and videoconference).
- Encourage control owners to raise their hands and ask for help if they encounter challenges in performing their controls.
- Communicate with control owners to emphasize on the importance of retaining high-quality documented evidence to support testing programmes.
- Promote open and ongoing communication with key service providers to identify the need to alter the current interaction model.
- Establish accountability and owners to deal with key issues and provide the ongoing status.
- Consider the latest SEC disclosure guidance on reporting the effects and risks of COVID-19 on your business, financial condition, and results of operations.

## Preparation for future controls assessments

Have you considered updating your control descriptions or creating alternative controls?

- Create or enhance existing policies and procedures to deal with the COVID-19 impact, inclusive of roles and responsibilities, timelines, and form of relevant artifacts.
- Evaluate affected areas for changes to people, process, and technology, and update controls accordingly.
- Engage with testing parties (testers and those being tested), including financial statement and service auditors, to understand/communicate expectations.
- Raise significant changes to risks and control environment to senior management and boards.
- Prepare for the likelihood of remote testing and the need for greater cooperation with both internal and external parties involved in testing.
- Consider the use of technologies, in particular communication tools and file-sharing platforms, to allow testers and business personnel to assess required information.
- Prepare a contingency plan in case the level of findings increase.

## Additional resources

For updates on COVID-19, information on new guidance, and resources available, please visit the following link:

- Deloitte COVID-19 homepage: www.deloitte.com/covid-19

[1] Committee of Sponsoring organisations of the Treadway Commission ("COSO") Internal Control Framework Components

# Contact us


**Ramu N**
Partner
ramun@deloitte.com

**Deepa Seshadri**
Partner
deseshadri@deloitte.com


# Acknowledgement


**Jaganjyot Singh**

**Taha Hussain**

**Jaykumar Trivedi**

**Arjun Prathap**