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**
- What is the effect of COVID-19 on the organization’s current risk assessment and risk landscape?
  - Revisit risk assessments, inclusive of fraud risks, and adjust for potential COVID-19 impact, for example:
    - 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, insider trading, theft of physical assets)
    - Monitor for emerging risks, and as they present themselves incorporate into risk assessment process

**Effective allocation of resources**
- Are resources allocated to the appropriate activities based on current environment? Are sufficient training and onboarding documents provided for individuals to serve as backups?
  - Identify and prepare back-up personnel for specific responsibilities, including executing control activities
  - Ensure that the back-up personnel identified have the required skills and competency to perform control activities, especially in cases of management review controls.
  - Review segregation of duties to ensure continued enforcement
  - 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

**Key service organizations reliance**
- What is the extent of business disruption for key service providers? Do additional oversight procedures need to be established during this period of disruption?
  - Contact outsourced service providers to evaluate their ability to continue to operate in accordance with established SLAs / KPIs, including monitoring of their service providers
  - Assess what temporary changes outsourced services providers have made to their control environments
  - Evaluate the extent to which additional oversight is required
  - Consider changes needed to what is currently in- vs. out-sourced based upon changes to your risk assessment
  - Formally document where certain decisions have been made to provide temporary relief
  - Revisit key documentation with service providers based on learnings gained during the current situation

**Remote access**
- Have users been appropriately provisioned remote access for their job functions? Have you established mechanisms to continue to monitor the remote control environment?
  - Scrutinise user access to assess only required access has been granted
  - 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
  - Pre-emptively review power- and super users for restrictions and adequate backups
  - Communicate with the business in order to reduce the volume of system changes requested to critical items only
  - Enhance monitoring of corporate network due to remote users insecure home networks
  - Leverage certification processes to gain insights on potential control frailties, people changes, and impacted processes in order to risk assess and respond

**Execution of controls and monitoring**
- Have decisions been made about required control modifications? Have you considered the need for enhanced monitoring processes over daily/weekly transaction controls?
  - Focus on how reviewers are evidencing review and approval through electronic means (e.g., emails, e-signatures)
  - Identify which automated controls are most susceptible to failure, due to COVID-19, or based on historical trends
  - Consider alternatives for controls that require physical observation (e.g., use of drones to conduct physical inventories by independent personnel)
  - Ensure appropriate monitoring controls exist and are operating effectively to mitigate any risks arising from a failure to operate the automated business controls
  - Be cognizant of the possibility that a number of controls that were in place earlier may no longer be effective or may require changes to continue to be effective.

**Linkage to COSO components**
- More can apply, based on our assessment

**Linkage to People, Policy, Process and Technology**

---

**Key questions**
- Consider the need for enhanced monitoring processes over daily/weekly transaction controls?

**COSO internal control framework components**
- Control environment
  - Risk assessment
  - Control activities
  - Information and communication
  - Monitoring

**Relevance and impact on other framework components**
- People
- Policy
- Technology
- Process
COVID-19: Control environment responses

Communication considerations

- Consider reinforcing the importance of control execution (e.g., newsletters, 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 emphasise the importance of retaining high-quality documented evidence to support testing programs
- Promote open and on-going communication with key service providers in order to identify the need to alter the current interaction model
- Establish accountability and owners for communicating key issues being dealt with and to provide on-going status
- Consider building enhanced reporting models for reporting within the entity as well as within the group to ensure timely receipt of essential information
  For example, financial and non-financial reporting metrics / exceptions to drive focus

Preparation for future controls assessments

- Consider updating your control descriptions or creating alternative controls

Impact on key governance documentation

- Identify what governance documentation would require change and prioritise such changes to best address business needs as well as allow changed control activities
- Consider the impact of such changed governance documentation on the IT systems
- Formally document changes to your business, certain decisions made, and the impact these may have on your governance, risk management and internal controls
- Consider how you plan to revert back to your original governance framework after COVID-19

Use of technology

- Changed roles within IT are carefully managed to ensure that developers do not have access to promote changes to a live environment
- Consider enhanced cyber-risks
- Ensure that the pressure to make changes do not drive the IT personnel to perform inadequate testing before they are allowed to go-live
- Assess the impact of dependency on third party vendors or external service partners in case they may not be able to deliver as expected
- Consider if automated interfaces will be monitored in a timely manner considering absence of some IT personnel

Relevance and impact on other framework components

- People
- Policy
- Technology
- Process
COVID-19: Control environment resources

Deloitte contacts

We're here to help. Please reach out to the key contacts below for more information:

- Vincent Sita
  Partner
  Controls Assurance
  visita@deloitte.com.au
  +61 439 744 788

- Janice Scott
  Partner
  Technology Controls
  janscott@deloitte.com.au
  +61 415 484 451

For updates on COVID, information on new guidance, and resources available to you, please visit:

- The future of controls: https://www2.deloitte.com/uk/en/pages/risk/articles/controls.html

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 8000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at https://www2.deloitte.com/au/en.html.

Liability limited by a scheme approved under Professional Standards Legislation.
Member of Deloitte Asia Pacific Limited and the Deloitte Network.
© 2020 Deloitte Touche Tohmatsu Limited