ASSESSING MANAGEMENT'S EFFECTIVENESS IN MAINTAINING EFFECTIVE INTERNAL CONTROLS DURINGTHE COVID-19 CRISIS

A QUICK CHECKLIST FOR AUDIT COMMITTEES

Organizations are moving at a frantic pace to manage risks during the COVID-19 crisis. These changes include organizational, process, and planned spending, all of which can impact the control environment. Boards, along with their internal audit functions, should oversee management's continuous assessment and management of these risks to help ensure the ongoing adequate effectiveness of the overall control environment.

Organizational Change Management

Ensuring changes in people and processes are considered in the design and effectiveness of internal controls is critical. The following are control areas the audit committee should expect the finance, internal audit, and IT areas to assess in this environment.

- □ Evaluate the frequency of risks assessments and ensure the alignment with pace of change relative to materiality, key accounts, and key controls.
- □ Consider if management risk tolerance has increased and tolerates a lower level of control effectiveness assurance (e.g. self-assessments).
- □ Consider how process changes are driving control design changes, including wording.
- □ Consider how people changes (reorganization, furloughs, and terminations) are impacting ownership, performance or review of key controls, and potential fraud.
- □ Consider how segregation of duty conflicts are managed with changes in people and process.
- □ Evaluate the use of public cloud based software such as Zoom, Slack, and SmartSheet, which team members may obtain for efficiency purposes. The free versions of these products can be utilized without going through the normal procurement process.
- □ Consider what annual controls (e.g. impairment and review of certain balance sheet accounts or covenants) should be done more frequently.
- □ Review with vendor risk management the critical SaaS vendors to ensure Service Organization Controls (SOC) reports are still valid in the updated work environment.
- □ Evaluate the timing and frequency of ensuring and validating key controls are effective (testing)
- □ Consider how management is assessing impact to key processes and controls of delaying capital expense investment projects including technology.
- □ Consider if any material changes in internal control over financial reporting will require disclosure in the next periodic report.
- □ Consider if any public disclosures about the actual and expected impacts of Covid-19 on their business and financial condition are needed, including how the Covid-19 pandemic may require additions or revisions to risk factor disclosures.
- □ Closely monitor and consider further restricting trading in company securities by insiders who may have access to material non-public information related to Covid-19 impacts.

IT General Controls and Security, and Privacy

Ensuring management is effectively managing general IT controls, and properly addressing security and privacy is critical.

Policy and Entity-Level

- □ Review work-from-home policies that require the use of organization owned and managed devices. Ensure requirements regarding security and privacy are addressed.
- □ Review personal device or Bring Your Own Devices ("BYOD") policies and consider disallowing access to organizational networks and data by devices that are not whitelisted.
- □ For personal devices that are allowed, ensure the hardware has appropriate security controls, the software is up to date, and these controls are supported by a policy.
- □ Require training on common security measures, such as protecting devices and password complexity.
- □ Ensure team members are trained on recognizing phishing attempts and have a way to report suspicious emails.
- □ Require training for handling personal information from both employees, vendors, and customers.
- □ Review policies for using only approved web meeting and data exchange sites.
- □ Ensure team members have an open line of communication with IT management and the help desk.

IT Change Management and IT Projects

- □ Ensure the IT change management process (including ticketing) has not been relaxed or compromised.
- □ Ensure controls for new builds of software or third party software implementations have not been relaxed (e.g. segregation of duties, user acceptance testing, etc.).

System Access and Authentication

- □ Require the use of VPN to access the network
- □ Ensure user access and provisioning controls have not been relaxed.
- □ Consider how management understands the effectiveness of risk management at third party service providers including physical security, IT security, data privacy, and confidential information protection.
- □ Ensure user access reviews are still being performed at appropriate intervals. This includes validating continuous effectiveness of access controls for both protection (e.g. terminated employees) and in alignment with organizational change of duties and remote work.

Privacy and Regulations

- □ Ensure controls on access and use of cloud shared drives such as Dropbox and Google Docs, which can lead to security and privacy related issues.
- □ Re-assess controls around applicable privacy regulations such as HIPPA and GDPR.

System Vulnerabilities

- □ Ensure system patches are applied regularly, and urgent situations like zero-day vulnerabilities are being addressed timely.
- □ Consider implementing penetration testing, or not forgoing already scheduled penetration testing.

Fraud (in addition to cyber threats otherwise mentioned)

Fraud risk may require a higher level of risk management considering increased change, remote work, and uncertainty.

- □ Is management continuing, if not increasing, messages around tone and doing the right thing?
- □ Consider if management is fast tracking new suppliers or other third parties.
- □ Ensure preventative and detective fraud focus is maintained, including allegation monitoring and investigation through appropriate and accessible methods such as a hotline.
- □ Ensure fraud is considered in risk assessment and management of change in organizational design, processes, and controls.
- □ Consider if there is an increased level of touch points with government officials, and if so, how FCPA and commercial bribery risks are managed.
- □ Understand how management is overseeing foreign operations in times of restricted travel.
- □ Validate continued physical oversight and security of key assets.

Returning to Work

As the economy begins opening up to full strength, organizations should consider the risks in their workforce and other stakeholders, returning to physical locations.

- □ Ensure management has assessed and is managing its preparedness to address health and safety procedures, this should include: implementing personal hygiene policies, such as hand washing; implementing distancing policies to prevent infection; and cleaning and disinfecting the workplace and preventing infection among those who clean and disinfect.
- □ Ensure management has assessed and is managing its preparedness to address applicable regulatory compliance and legal issues.
- □ Ensure management has assessed and addressed human resource issues including: health and safety policies for employees, identifying and protecting at-risk employees, informing employees of possible exposure at the workplace (contact tracing), and protecting confidentiality of infected employees.
- □ Ensure management has assessed and addressed health-related issues including: availability of personal protection equipment, testing to identify currently infected employees, testing to identify previously infected employees, and vendors and supplies for cleaning services.
- □ Ensure management has assessed and addressed operational impacts including: physical modifications to workplace for social distancing, potential reduced productivity, and increased costs related to adapting workplaces for employee safety.
- □ Understand how management will continue overall communication around its focus on the welfare of employees and stakeholders.

References

COVID-19 and Internal Audit: Preparing for the New Normal in 2020 and Beyond (The IIA, Internal Audit Foundation, and AuditBoard).

COVID-19 Operating in the "new normal" – A backdoor to increased fraud risk? (Deloitte).

Evolving Cyber Risks in a COVID-19 World (The IIA, Internal Audit Foundation, and Wolters Kluwer).

How boards can approach the Covid-19 pandemic (Governance, Risk, and Compliance Corporate Secretary).

Audit Executive Center COVID-19 Quick Poll #3 (The IIA).

NACD COVID-19 Resource Center

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

NACD

The Institute of Internal Auditors