TX Office: (817) 416-6842
NV Office: (702) 565-2727

Kral Ussery
Certified Public Accountants
Advisors - Litigation Support - Internal Audit

April 27, 2020

The New Landscape of IT Internal Controls

Dealing with a home office environment

By Ann Simmons, PMP
Technology Director, Kral Ussery LLC

Information Technology controls are like the Chicago mass transit system (the buses, subways, trains and elevated trains). When the components are well maintained and running, schedules are met, and Chicago is not experiencing one of its 10-year blizzards, we don't think of all the components that are working together for successful transportation. The shift in remote working, as a result of COVID-19, challenges and tests the structure around previously implemented controls which may ultimately impact shareholder value.

This article identifies categories impacted by the structural shift that is occurring with remote work and considerations for internal controls. Also, refer to our COVID-19 ICFR Questionnaire of control considerations, including IT.

The Speed of Change is Rapid

In the last three weeks, here are examples that occurred to colleagues as they sat at their corporate desks one day and were forced to work remotely the next. Imagine yourself in one of these discussions:

- The IT Director came into my cube, gave me a box with a new computer and instructions to contact the technical support team to "get things up and running". I had no idea of where I would be working, how to connect my PC to my home network and where I would get the critical files for my job. What is a Zoom meeting anyway?
- My company decided to have all employees in the Customer Service Department ("my department") begin working remotely the next day. Mentally, I started a conversation that sounded like:
    - I don't have a home office as I live in an efficiency apartment.
    - My spouse is also required to set up a work space in my home and we only have a single kitchen table.
    - Do I have an internet connection that is sufficient to support both of our work?….and this was just the beginning of the mental questions.
- A large mental health partnership specializing in programs in the area of addictions could no longer support a model to care for patients onsite. These were group programs involving at least two counsellors per session. The patients and their

cases are extremely confidential as are the discussions in the group sessions. The program director was overheard working with the staff in trying to put together a remote delivery model that was effective and safe.

Is This Structurally Different?

For years, there have been pockets of professionals who worked remotely - consultants, help desk support staff, sales professionals, fund raisers, trainers, technicians, etc. However, the critical distinction is the word "pockets" of professionals. As internal auditors, we assess the design and operating effectiveness of internal controls, including monitoring for remote workers based on the type of work and their access to critical and sensitive information. But with COVID-19, the exception is now the norm and working remotely is not a luxury or an option - it is a requirement. Companies have understandably responded rapidly and deliberately as people are working from home offices. However, it is critical not to lose sight of the associated business risks and following considerations:

Business Continuity Planning: The pandemic triggered the need for business continuity in a real sense. Was the migration to remote working based on a documented and tested Business Continuity Plan?

- If a plan existed for a company, was the plan effective in the execution?
- If no plan existed, is there a process for identifying "gaps" in business continuity with remediation? For example, we know of one company where no plan existed and once the HR staff began working remotely, they had no access to hardcopy personnel files that were "left behind" in the offices. This company needed to engage, at great expense, a third-party scanning company to provide access to the records.

A complete Business Continuity Plan includes the return to work in the original setting. Now is the time to develop this plan. The "return or reentry" plan should include technology, timing, people, records and process.

First Things First: While numerous internal controls need to be evaluated, updated and adjusted to ensure protection of computing assets and information, four generally rise to the top:

- Remote workers are now rapidly accessing corporate assets for critical and confidential functions. Access and monitoring are critical. The network technical staff should be vigilant in implementing and monitoring access.
- Check and double check who is accessing the network and computer assets. With the rapid movement toward remote access, now is the time for a well-placed and "smart" hacker to penetrate computers. If necessary, increase layers of security for access.
- Beef up the help-desk to include technical Levels 2 and 3 support. Encourage use of the help-desk as the correct answer with appropriate governance to avoid "workarounds".
- Evaluate the benefits and costs for implementing "in-transit" encryption for critical and confidential data.

Every home office is now a "tiny IT organization": The movement toward the "tiny" IT organization may have begun with the advent of the PC, or with "end user computing", or the decentralization of the IT organization, or with the outsourcing of IT to third parties, thus resulting in the blending of business and technology processes. Companies are now asking every one of their employees who have moved to remote working to be a network engineer, a software engineer, a security expert, a PC technician, a developer, a meeting facilitator, a help-desk analyst (Level 3 no less) and a CIO. In a way, we may have partially prepared our employees but many of the structures that had been established must now be reviewed, revised, communicated and tested. Here are a few considerations that should be addressed:

- How are the prior Acceptable Use Policies impacted and what has changed?
- How is confidential organizational data protected, including detection of unauthorized access to data?
- What is the impact to the complexity and nature of incidents in the area of incident detection and resolution?
- Are there additional provisions (security, physical access, confidential hardcopy data) that are unique to remote work?
- How will we integrate online meetings into our culture?
- What is the spending tolerance for remote office requirements?
- What will be the need for new standards and practices specific to remote work?

Conclusion

Remember that your design of controls must be in line with business operational changes, ideally in a real-time manner. Otherwise, companies jeopardize shareholder value against errors and fraud, including cybersecurity risks. We will continue to explore the IT challenges, risks and possible mitigation actions related to remote work in future articles.

*****

Ann Simmons is the Technology Director of Kral Ussery LLC, a public accounting firm delivering advisory services, litigation support and internal audits. Ann works with security protocols, development processes, system access controls and rights, application change authorization, and network and infrastructure security. Contact Ann at ASimmons@KralUssery.com.

Kral Ussery LLC serves US public and private companies to protect and grow shareholder value, as well as non-profits and governments with internal controls and in combating fraud. We assist entities with governance and in all matters relating to financial reporting, including SEC compliance, internal controls testing and remediation, IT general controls, IPO readiness, M&A transactions, and US GAAP. Visit us at www.KralUssery.com.

This is an article from the Governance Issues™ Newsletter, Volume 2020, Number 2, published on April 27, 2020 by Kral Ussery LLC.