Group 5: My Pham, Reshma Maliakkal, Sukruta Srinivas, William Marty, Cody Blanchard

Professor Joseph Mauriello

ACCT 6336 - IT Audit and Risk Management

13 March, 2019

Assignment 2 - IT General Controls

Logical Access

1. Information Technology General Controls Overview

Information Technology General Controls (ITGCs) are controls that are applied to the Information Technology (IT) environment in areas such as “applications, operating systems, databases, and supporting IT infrastructure” ("IT General Controls Audit | IT Audit And Compliance" 1). The role of ITGCs in the audit procedure is to understand the existing IT environment, perform the walkthroughs, interviews, and documentation reviews for the currently existing environment, review how appropriate existing controls are, and finally confirm that these controls accurately assess control operating effectiveness (Amasaki 6). ITGCs, typically used within a business to aid with disaster prevention, planning, and recovery, are required to be in compliance with The Sarbanes-Oxley Act of 2002 (SOX) ("SOX ITGC | Implementation, Compliance & Reporting" 1). SOX itself does not have clearly defined standards for its ITGCs requirements; however, other IT process standards such as COBIT 4.1, COSO, and ISO 27001:2013 are usually used as the framework for ITGCs ("SOX ITGC | Implementation, Compliance & Reporting" 1). The most common areas of ITGCs include logical access, system development, system change, and computer operations.

Logical access controls are defined as “interactions with hardware through remote access” and include features such as identification, authentication, and authorization protocols ("What Is Logical Access? - Definition From Techopedia" 1). Logical access controls allow a business to protect its hardware from unauthorized access by having methods of identifying and screening the users that can access the business' data, ranging from password programs to advanced biometric security systems ("What Is Logical Access? - Definition From Techopedia" 1). Systems development is the process where a new software application or program is planned, analyzed, designed, implemented, and maintained ("Systems Development | Software Application | Development" 1). The systems development life cycle allows a business to thoroughly analyze a software application or program prior to implementation in order to prevent potential loss of service or security vulnerabilities. Systems change management general controls include new system implementations as well as the upgrades and patches; system change management also ensures that there is the "segregation of incompatible duties exists within the manage change environment" (Miron 13). System change general controls are beneficial to businesses because they allow "only appropriately authorized, tested, and approved changes" to be made (Miron 8). Computer operations can include batch job processing, the monitoring of the success or failure of jobs, incident handling, and backup or recovery procedures (Amasaki 14). All of these ITGCs allow a company to rest assured knowing that they have protected their data, and that their IT processes are secure.

2. Associated Risks of Logical Access

As there have been significant technological advances in the past decade, criminals have gained knowledge of IT to become much more creative and clever in identifying ways and new tools to break into weak systems. In fact, Singleton claims that logical access to systems is not only one of the top concerns for management in any audit, but also among the five areas of IT general controls that need examination in every financial audit. Experts believe that criminals are concentrating more on IT crimes than "traditional street crimes" (Singleton). Singleton also provides that current or former employees account for 80% of all harmful activities, according to the Computer Emergency Readiness Team (CERT) and the industry security analysts.

Lack of sufficient authorization, authentication or internal controls can lead to multiple logical access risks. Many companies may not pay enough attention to their system security and set weak or unsophisticated passwords. IT-savvy criminals may be able to attack computer systems of an organization and change or steal large amounts of data. Their ability to get access to financial applications such as payroll or intellectual property may create fraud. If the company has incorrect information, users including management will use those data to make poor business decisions ("IT Audit Risk & Controls Overview" 13). The inappropriate access to key production applications will also disrupt the business processes. Additionally, their access to the organization's network will not only interfere the business processes, but also negatively affect the reputation of the company ("IT Audit Risk & Controls Overview" 13). Thus, as the risk is higher, the organization needs to have more complex and secure access as well as "additional layers of access controls" (Singleton).

Since segregation of duties (SOD) is a major factor of internal controls, internal auditors need to review the effectiveness of their company's SOD. Lack of segregation of duties may include access from inappropriate departments, employees or unrelated staff members. During their audit process, if their logical access does not indicate SOD's effectiveness or comply with SOX requirements, errors are most likely to be undetected. As a consequence, the organization becomes vulnerable to the possibility of fraud and increased external audit fees ("Segregation of Duties and Logical Access Guide" 11). In order to prevent the company from facing legal issues with respect to regulatory requirements, IT general controls such as logical access need special attention because compliance with SOX regarding technology can be challenging to organizations.

3. Control Objectives of Logical Access

The objective of implementing logical access controls is to restrict access to certain systems within an organization to specified individuals. The specific control objectives depend on the organization, but some goals management may wish to achieve through logical access include identification of individual users of IT data and resources, authenticating that the users are actually who they appear to be, and that those authorized can only perform certain functions in the system.

Identification of users of IT data and resources is one of the key components of logical access controls. The most common method of identification of users is the use of usernames and login credentials (Cascarino). Usernames allow the system to identify who and when people attempt to access the system, creating an audit trail as a result. This audit trail can later be used if someone gains unauthorized access to a system, allowing auditors to trace and identify the offending party. It also allows them to revert harmful changes the unauthorized user made if they track those changes.

Authentication is the process of determining “whether individuals are who they say they are” (Cascarino). This is done through ensuring that the specific holders of those accounts are the only ones who can access them. The most common method of authentication is the usage of passwords, in which the user must know the combination of characters in addition to the username to access the system. Other forms of authentication include key cards, and biometrics (Singleton). Finally, two-factor authentication is rising in popularity as an access control. Many accounts can be compromised if they rely solely on passwords, as they are vulnerable to bad actors guessing the password, overhearing it in conversation, or gaining access to them through a data breach (Cascarino). Two-factor authentication counters these security weaknesses by forcing users to know the password and something else--a code sent to an app on the user’s phone, for instance--to gain access to the account (FOS).

Authorization is an objective that is obtained when both identification and authentication have been verified, because the combination of the two proves an identity (Darril). When authorization is established, it ensures that a user is accessing authorized resources intended for that user. In contrast, without authorization there would be no way of differentiating users when they have access to a system.

Resources that might require an administrator to view or change will not be defined and by default everyone will have the same access and the rights to everything, creating a major risk.

Logical access controls should restrict access to certain systems only to users who have proper authorization to use those systems. Employees should not be able to perform certain tasks that are incompatible, such as the person writing checks also performing the bank reconciliation. Restricting user access also prevents employees from having more responsibilities than they should have, such as “having unlimited access to assets, accounting records, and computer terminals” (University of Utah). Through the prevention of incompatible duties, companies can enforce proper segregation of duties and prevent fraud.

4. Preventative, Detective, and Corrective Controls of Logical Access

Preventive controls are the first line of defense which strengthens the system against incidents and helps minimize the vulnerabilities (“Preventive-Detective-Corrective Internal Control Model”). They are proactive controls that help to ensure departmental objectives and reduce the frequency of occurrences of undesirable events (“Are There Different Types of Internal Controls?”). Preventing frauds and errors is more cost effective than detecting and correcting the problem. An example of preventive controls is segregation of duties. Duties are segregated among different people to reduce the risk of errors or inappropriate actions. Tasks such as authorizing transactions, recording transactions and handling related assets are divided. Another example is to ensure that management provides authorization with employees to perform certain activities and to execute certain transactions within limited parameters. Management also specifies those activities or transactions that need supervisory approval before they are performed or executed by employees. A supervisor’s approval signifies verification and validation that the activity or transaction conforms to established policies and procedures. With security of assets, a preventive control is applied to restrict access to devices, securities, software inventory, cash and other artifacts. Moreover, maintaining a count of assets is crucial along with validating it with the control records (“Are There

Different Types of Internal Controls?"). While ensuring preventive measures for data and assets, the company can check for password controls such as length, complexity, expiration and history, conform to organizational standards or best practices. The organization can ensure that patch management is in place, and updated, new patches are applied timely to remediate known vulnerabilities. Sensitive data should also be checked to see if they are encrypted within databases, on hard drives, and during network transmissions (Whitaker 16-18).

Detective controls are second line of defense which identifies and exposes security violations after they have occurred, or provides information about the violations as part of an investigation. These controls disclose specific errors by comparing occurrences with pre-established standards and policies ("Preventive-Detective-Corrective Internal Control Model."). Some examples of detective controls are comparing different sets of data to one another, investigating and identifying differences. Thus, to ensure accuracy and completeness, management must review reports, statements, reconciliations and other documents to check for consistency and integrity ("Understanding Internal Controls" 12-16).

Corrective controls are used to reverse effects of errors detected in the previous steps. Once the risk has occurred, corrective controls help mitigate the damages caused by it ("Preventive-Detective-Corrective Internal Control Model"). Some examples of corrective controls are to determine a well drafted incident response plan which can be materialized when risk/damage is identified, to ensure that proper root cause analysis is performed after every incident or problem, and further to provide a permanent fix by taking immediate actions in terms of providing bug fixes, patches and reducing mean time to resolution (MTTR).

5. Tests of Control Recommendations

One major test auditors can use for identification is to ensure each user has a unique ID. This can be done through an interview of key personnel in the company, by reviewing the company's documentation of their controls, or by observing a user accessing their account. A system that relies on group usernames is far more prone to security breaches than one with unique IDs. Auditors should also review the audit trails generated by the system to see if identification of the user is included in the audit trail. Some information that should be included in the audit trail includes usernames, time and date of access, location of access, and the content of the changes the user made in the system (Cascarino).

Once the auditors assess the level of risk in an environment, they develop an audit plan for testing the control. When it comes to authentication, there are several controls that a company may implement for logical access. In an environment that uses a Windows server with Active Directory for domain and application authentication, auditors may want to test against default system accounts, password complexity, and effectiveness of two-factor authentication, just to ensure that the processes and protocols behind the authentication mechanism are effective. Another technique auditors may use for Windows machines is utilizing auditing tools like "DumpSec", which checks local accounts, password configuration, audit log settings, and more (Singleton).

To reach reasonable assurance for the authorization objective, auditors must prove that a specific resource or function is restricted to the right personnel. Authorized access must demonstrate to be associated with an established authorization level and show for a mechanism that checks for authorization level before allowing access to resource. According to Singleton, depending on the level of risk assessed in an audit plan, auditors may perform a simple test of ensuring authorization is at least working in a low risk environment. In a simple test, auditors may evaluate the user account access level to ensure that appropriate access is associated with user's job duties, but also check to see if processes are working as designed. For higher risk testing, Singleton notes that an entity should have a combination of controls to test and uncover flaws in the authorization and holistic logical access process.

In our modern, data-driven world, physical controls are not efficient enough to protect companies from harm. Logical access controls are necessary to keep a company's data safe from identity theft or alteration by outside parties. The use of identification, authentication, and authorization can help companies identify who is accessing their systems, when and what changes they make to their data, and ensure that those individuals have proper clearance to access those systems.

Works Cited

Amasaki, Sugako. " Information Technology General Controls (ITGCs) 101". 3 Dec. 20015.

“Are There Different Types of Internal Controls?” *Audit, Risk, and Advisory Services*, www.vanderbilt.edu/internalaudit/internal-control-guide/different-types.php.

Cascarino, Richard. “Logical Access-Control Audit Program.” *Wiley Online Library*, 2012, onlinelibrary.wiley.com/doi/pdf/10.1002/9781119203728.app3.

Clarke, Isaac. “Control Objectives & Activities: What Are They? What's Appropriate?” *Linford & Company LLP*, Linford & Co LLP, 17 Feb. 2019, linfordco.com/blog/appropriateness-of-control-objectives-and-controls/.

Climbing New Heights, Association of Healthcare Internal Auditors. Microsoft PowerPoint presentation, https://www.appliedtrust.com/services/standard/sox.

Darril. “Identification, Authentication, and Authorization.” *Get Certified Get Ahead*, 25 Aug. 2015, blogs.getcertifiedgetahead.com/identification-authentication-authorization/.

Kenton, Will. “Detective Control.” *Investopedia*, Investopedia, 12 Mar. 2019, www.investopedia.com/terms/d/detective-control.asp.

“Fundamentals of Information Systems Security/Access Control Systems.” *Fundamentals of Information Systems Security/Access Control Systems - Wikibooks, Open Books for an Open World*, en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Identification_Authentication_and_Authorization.

“IT Audit Risk & Controls Overview.” Buchbinder, 12 May 2016, www.buchbinder.com/wp-content/uploads/2016/05/MP-NFP-Event-IT-Presentation-5_12_16.pdf.

"IT General Controls Audit | IT Audit And Compliance". Schneiderdowns.Com, https://www.schneiderdowns.com/it-general-controls-audit.

“Manage Risks with Preventive, Detective, and Corrective Controls.” *CFO Career Planning Tools*, 15 Oct. 2013, www.cfocareer.com/manage-risks-preventive-detective-corrective-controls/.

Miron, Ben. “Understanding IT General Controls.” Association of Healthcare Internal Auditors, 9 Sept. 2008.

“Preventive-Detective-Corrective Internal Control Model.” *Scribd*, Scribd, www.scribd.com/doc/63958553/Preventive-Detective-Corrective-Internal-Control-Model.

“Related Websites.” *Department of Internal Audit*, University of Utah, audit.utah.edu/segregation_of_duties.html.

“Segregation of Duties and Logical Access Guide.” KnowledgeLeader.

Singleton, Tommie W. “Mitigating IT Risks for Logical Access .” ISACA, www.isaca.org/Journal/archives/2010/Volume-5/Pages/Mitigating-IT-Risks-for-Logical-Access.aspx.

Singleton, Tommie W. “What Every IT Auditor Should Know About Access Controls.” University of North Carolina Wilmington, 2008.

"SOX ITGC | Implementation, Compliance & Reporting". Appliedtrust.Com.

"Systems Development | Software Application | Development". Elinkdesign.Com, 2019, https://www.elinkdesign.com/web-services/application-development/systems-development-.

“Two-Factor Authentication | FOS : Bank Internal Audit and Compliance Consulting.” *FOS*, 26 Oct. 2017, fosaudit.com/two-factor-authentication/.

“Understanding Internal Controls”. www-bfs.ucsd.edu/blink/ocbfs/acc/UnderstandIC.pdf. University of California, San Francisco. Microsoft PowerPoint presentation.

"What Is Logical Access? - Definition From Techopedia". Techopedia.Com, https://www.techopedia.com/definition/23926/logical-access.

Whitaker, Chase. *Practical Guidance for Auditing IT General Controls*. Ahia, 2 Sept. 2009, www.resourcenter.net/images/AHIA/Files/2009/AnnMtg/Handouts/C7.pdf.