The importance of information technology auditing

Technology

Information technology auditing is important to the financial auditor and to the financial statement audit because IT is the foundation of today's accounting systems. IT audits are crucial for ensuring that a company's financial statements are a representation of the company's position and that the system used to compile the statements is operating properly and producing accurate statements.

IT auditing allows the auditors to provide a more effective financial audit because it provides the auditor with the processes and information that the client used to prepare the statements. IT auditors have three objectives; to prove " the confidentiality, Integrity, and availability of data". Both the IT auditors and the financial auditors can decide what processes best ensure reliability of the financial statements. (Wood, Brown, & Howe, 2013) There are five management assertions that are considered during all types of audits; existence, completeness, rights and obligations, valuations, and auditing procedures.

IT audits go beyond proving that the company's financial statements pass all five management assertions, instead they delve beneath the top layer of information provided by the company and search within the software to find whether the system the company uses to document all of their financial fights against intentional and unintentional misstatements. For example, when an auditor is proving existence they will typically look at the sales Journal to see what item was sold and then prove that the Item was actually sold.

An IT auditor will " break Into the system" and read the code that proves that when a piece of Inventory Is bought the system registers It In he sales Journal and In the Inventory Journal. He Is responsible for ensuring that " all necessary and required controls exist". When proving completeness, an IT auditor is responsible for verifying that the controls in place are working properly. Considering the example mentioned above, to prove completeness, instead of simply verifying that a control exists for making the necessary changes in the sales Journal and inventory, the auditor would have to prove that the appropriate changes are actually made. Wood, Brown, & Howe, 2013) (Audit Objectives and Evidence, 1999) Rights and obligations attest to the company's legal status of its assets and liabilities. An IT auditor would use this assertion to prove that the Information used in the systems Is legitimate and that there are controls In place to maintain the Integrity of the Information Inputted. A financial auditor considers the valuation assertion as a way of proving accuracy within a company's estimates that are used as the corner stones of the valuations of their assets and liabilities.

An IT auditor would assess the tables, the design and accuracy of spreadsheet models and the integrity of repository data source". Financial auditors substantiate that accounting procedures are in place by examining who performs the task, such as preparation and posting of end of period adjusting entries, and that the task was completed. An IT auditor would focus on determining whether such task was performed by the person that was actually assigned the task. Wood, Brown, & Howe, 2013) IT controls relating to the above assertions, as well as all other IT controls, need to be assessed regularly in order to guarantee that the company is protected against

misstatements and weaknesses within their system. Over time, companies have become more and more IT integrated. This means that companies face new challenges as the demand for software applications increases and more software products are placed on the market, before companies did all of their financial work by hand.

It was normal to take out a calculator and a number two pencil and begin a tally when counting inventory. Today, companies use software that counts the inventory that is being purchased and in turn deducts it out of the outstanding inventory balance. With the new technology, companies are challenged to find ways to protect themselves from errors and provide their clients with integral financial statements. Because of this " newer" challenge, IT audits are vital to ensuring that the company has the correct controls in place to cover all of the bases.

Control environment, one of the concepts of the COOS framework (Committee of Sponsoring Organizations), is one of the areas that IT auditors investigate when considering the completeness of the company's controls. Control environment is set by the tone at the top of the organization; by managers, and board members. " It is the foundation for all other components of internal control, providing discipline and Truckee" (Internal Control Integrated Framework, 1992). A study examining 490 small firms that reported material weaknesses in the first year of the SOX compliance determined that IT affects the overall control effectiveness of a company.

The study found that a weak control environment will affect the four other parts of the COOS framework, confirming that control environment is the

cornerstone of the COOS framework. Additionally, the study established that a company with weak IT controls frequently in turn causes non-let related misstatements and weaknesses (Claim & Watson, 2009). The study helps prove that IT controls need to be assessed on a regular basis to ensure that the company's software is functioning properly and to help eliminate material weaknesses and misstatements.

Software companies design their products to help protect the intended user's privacy and information. In order for a company to be interested in purchasing the software, the software, at a minimum, has to include security controls. One security control that a software company would provide the users with is the administration ID and passwords. This means that after the software is bought, one person within the many has the ability to have full access to the software. Typically, an IT personnel whomever they feel necessary.

Companies will have the ability to set up more than one administrator and password during the initial configuration. (Wood, Brown, & Another security control that would be provided with the software is the end-user IDs and passwords. These IDs and passwords will be provided to the personnel who use the software to complete their tasks. The administrator will be responsible for setting up the IDs and passwords. (Wood, Brown, & Howe, 2013) Access rights is another security control that should be built into the system.

This allows the administrators to restrict and provide access to the different functions within the system as is necessary for the personnel to complete

their appropriate tasks. This is a very important security control because it can help prevent material misstatements by disallowing any inexperienced or unauthorized personnel from entering a section of the system that they are not trained or qualified to be in. (Wood, Brown, & Howe, 2013) The system should be designed with user management controls.

User management controls are put in place to remain current on which user has access to what parts of the system. It also helps manage removing and disabling users from the system as well as modifying current user access within the system. The administrator will be the one to maintain this part of the system. (Wood, Brown, & Another security control that should be building into the accounting system is the ability to create security logs and audit trails. The administrator will be able to set up this control to their company's standards.

An audit trail is also imperative when ensuring security within the company. It is imperative that management can track the user's movement within the system to protect them from risk. If a user manages o gain access to an unauthorized part of the system and make unauthorized changes, the logs will prove which user made the changes. Knowledge of any failed login attempts can alert the administrator to possible security issues and allow them to be proactive and put additional controls in place to prevent unauthorized access. Wood, Brown, & Howe, 2013) Application controls that are built into the software system affect the following business cycles; revenue cycle, expenditure cycle, inventory cycle, and the payroll cycle. The business cycles cover the same five major application control types; edit checks, validations, ululations, interfaces, and authorizations. Several

examples of the application controls that relate to the business cycles are logical access controls, date entry/field validations, workflow rules, and field entries being enforced by predefined characteristics.

The systems typically need initial configuration and occasional maintenance to ensure the controls are being used correctly and efficiently. Discussed below are some of the ways the application controls affect each of the business cycles. (Wood, Brown, & Howe, 2013) In the revenue cycle, edit checks involve checking to make sure that the correct field o typed a letter in a place that can only contain numerical values. The system would alert the user to the error. Edit checks are not inherently placed in the system. The administrator is responsible for defining the content and format that should be entered into the system.

Validation controls include verifying customers and verifying credit limits. The administrator would assign credit limits for each customer. The software would then notify the user if the total order amount exceeded the credit limit. Similarly, the system will have steps for the administrator to input the pertinent customer information for each of the application controls and then allow the administrator to run the automated controls to determine if the data is accurate. The expenditure cycle allows for a different type of validation check.

The " three-way match" which compare three different documents to determine if the information matches on every document. For example, consider a check to a vendor. A " three-way match" would involve reviewing the receiving report, purchase offer, and invoice before the check is actually

written. Another control to consider in the expenditure cycle is the logical access control. Again, these are not initially configured when the software is provided to the client. It is the responsibility of the company to assign the appropriate access to each user.

Consider that the master vendor file is not restricted. This has the potential to cause mayhem; anyone who has access to the program can access this file and change it as they see fit. The master vendor file should not be accessible to all employees. The administrator is responsible for assigning the users the appropriate access for the system. (Wood, Brown, & Howe, 2013) Another control the company should be concerned about when discussing the expenditure cycle, is the workflow process. The workflow process involves electronic routing and the signing off of expenditure requests.

This control has the possibility to limit fraud and prevent misstatements from occurring because it recognizes the need for certain documents and tasks to be completed. One example of this is having the system alert the user to a purchase order not being approved, if applicable, when the user tryst to print the purchase offer. This control requires that an individual reviews the purchase offer and sets their approval status to " approved" before the purchase order can be printed. This control is one that needs to be set up by the administrator upon initial setup of the system. Wood, Brown, & The inventory cycle involves a lot of costing information to be entered into the system by the users. As with anything inputted by the users, this opens the door to errors. These errors are sometimes related to input errors or incorrect costing information. System reports are one control that the

software has that can help eliminate these errors. The system reports are inherently programmed into the software but the user needs to " print" the report themselves. The administrator can also activate a control hat requires the user to print the report once weekly or as they see fit.

Another issue that can arise in the inventory cycle is the variances of raw materials. Inherently programmed within the system are controls that the administrator can set up to alert on the variances. As mentioned above, application controls under the previously mentioned business cycles also apply to the payroll cycle. For example, as with the expenditure cycle, application controls can be put in place to prevent unauthorized changes to the master files. The system administrator can assign and restrict access to all of the efferent parts of the system.

Additionally, one risk that can be eliminated by application controls specifically for the expenditure cycle is the risk of inaccurate tax records due to lack of updating the file or improper calculations. The administrator can set up a control that requires the management to sign off on a report of the tax records to ensure accuracy. Like financial audits, IT audits are essential to ensuring the accuracy and reliability of a company's financial statements. Software systems are designed with certain application controls that will allow the users to protect their company from the threat f material weakness and misstatements.

However, it is up to the management to ensure that the company is properly using the software. With proper use of the software and occasional IT audits,

the company will be able to enhance its investors' and clients' trust in their financial statements.