Auditing Information System : Delivery Product Service

Purwoko

Abstract - Purpose of the research is to ensure the securities of information system asset and to ensure if informa-tion system support the operational and data collected was valid. Research method that used in this research were library studies and field studies. Field studies such an observation, questioner, and inter-view. the expected result are founding the weakness of security management control, operational man-agement control, input control, and output control of risk happened in the company. Conclusion of this research are the system on the company work good and there's no potential risk happened and make an impact to the delivery process of information system.

Index Terms - Auditing Information system, Delivery product process.

1. Introduction

Business development on Indonesia's company become more competitive and many companies trying to be survive at this business flow and so with information technology nowadays. Information system used to support the company's operational specially in the internal control.

According to Malkawi et al. [2], auditing information system being a central to the effective organizational management and have a three basic challenges in its current practice such as a limited guidance of management of scope, ambiguous linkage to related ICT development process, and the lack of methodology approach. According to Keizer [5], Hirth [4] there are some benefit of using IA in Auditing Information system process, IA will help the company to improve the internal control and they help the company to increase the likelihood that it will achieve its objective and help to reduce the fraud, helps to properly validate and continuously improve control and serves as vital source of management talent to delivers a future leader of organization, and they also have a innovative thinkers who can meet a wide range of challenge that related to the governance, risk, and compliance.

This research will take a place in PWP, Ltd that focus on road transportation, especially for delivery of goods with truck. This research needed to asses if the internal control in the company can handle the risk happened.

2. Research Method

The research method that used in this paper are library studies, field studies, and analysis of data. The library study was done by getting some information from book, website, and science literature. Another method is field studies that were done by doing an interview, observation to the company, and making a questioner. Analysis of data was done by checking the validity data with the theory.

3. Literature Review

According to Abdolmohammadi and Boss [1], IT audit become necessary to maintain a competitive advantage of the company and also help the company to realize the benefit they will get in a period. IT audit will utilize their auditor to facilitate the design, implementation, and audits of system control in the company, and all of the working are based on computers aspects of information system, it also suggest the auditor must process specialized knowledge when they did their job. But there's always a training for technical knowledge and use as a proxy in the organizational knowledge. The skill of the IT auditors are extensive because they must be an auditor and IT professional, however even they have any skill in auditing, the employees need to join test that will help the employee how far their skilled on working. The increasing of IT audit will decrease the dependence happened in the company on their department of IT audit function to the consultant.

According to Verschoor [7], Now, an internal auditing will represent a cutting-edge and it works when an internal auditor and author have a special experience in IT audit. IT audit divided into two large activities, first the adding value through consulting service, mainly giving an advice but perhaps it leading the organization to be stronger with more vigorous risk management system and must be tuned to avoid the loss of objectivity and independence necessary to provide the opinion about the process, data, and information. Then, IT audit will containts overall objectives based on perspective, IT governance, and the performance in IT audit.

According to Ortiz [6], in audits, both of internal and specific IT assets are essentially underspining in the information security, and viewed mutually to the protection companies. Audit committee and IT auditor are sensitive to cognizant the roles due care and due diligence play within an organization respect. The personnel from Internal Audit and IT Audit department will recognize the importance of conveying the best practices information to the executive leadership, stakeholder, and corporate managers.

According to Yun [3], IS audit refers to the whole of audit process in the company which are to organize and plan the auditing project and implement it if there's any information wheter the information must be safe, reliable, and effective. IS audit will be divided into three phases, first in Auditing preparation phase. In this phase, the IS audit will be clarification the audit subject, identified the targets, determine the audit objects and scope, and also formulation the auditing plan as well as auditing service agreement. Then the second phase is Auditing Implementing phase, it will collect and analyze the data and information, determining the auditing test method, looking up the policy, and test all the control. The

last phases will be auditing finishing phase, which evaluating the test result, communication with managers, and writing up the auditing report.

4. Audit Plan

Before doing audit in the information system delivery, we can make an audit plan to get a description about the ongoing procedure by choose the scope and purposes. The scope of audit will be an internal control and application control, where the general control will restrict in the security control and operational controls, then for the application control will take an input control and output control. The purpose of this audit IS are :

- Ensure the asset security of information system in the company
- Give the faith of asset information system include hardware, software, brainware, dan it own data that will support the operation
- Ensure that transaction data was valid
- Make sure that the information are valid and complete and can be distributed to the right person

Problem happened and recommendation in Security management control. There's some problem that found in the management control of the company:

There's no alarm in the access door to the asset room to anticipate the stalker. Risk: if there's no alarm, it could make a probability there's a stalker go in to robbed the asset without anyone knows. **Recommendation**: better if the company uses an alarm to detect intruders

There's no fire extinguisher in asset room. Risk: there will be no warning if there's any fire. **Recommendation**: get the fire extinguisher in the strategic place, especially in the different asset room

There's no warning to change the password periodically. Risk : it will make the external user can access the illegal thing into the application system. **Recommendation**: it better if the employee change the password periodically to save the data. There's no recovering plan if the disaster happen in the company. Risk: when there's any disaster happen and make the operational down, it will make any loss to the financial part in the company. **Recommendation**: Company make a disaster recovery plan that will divide into four , which are emergency plan, backup plan, recovery plan, and test plan. For emergency plan, company has to know where they should contact, what action they have to do, and the procedure needed. In back up plan, company has to get a back up in every data information. In recovery plan, company have to make a procedure to make a recovering in the operational and system. Then, to ensure if the emergency plan, backup plan, and recovery plan are appropriate with the recovering plan, the company have to do a test plan.

Company get a control in operational management of the company, such:

- Company make a training for the employee to operate the computer system
- Company will describe the job description to the employee about how to operate the computer
- Company will maintain the hardware and software periodically
- Company have a location setting in computer physic
- The hardware software now are support the ongoing system in the company

But there's also a problem happened in the operational management, Company doesn't have any brain ware to solve the problem happened in the hardware and software. Risk: when there's error in the hardware and software, there will be none technician will solve it. Recommendation: build the technician to solve any crash in the hardware and software.

An input control in the company such as:

- Company have an input data procedure
- Company have any roles in authorized the input data
- Company have any procedure to log on into the system
- There's any restriction in name and column that can be filled by the special employees
- Company have to check about the probability happened when there's an eror in input data
- There's any warning if the system haven't fill properly
- Company have any procedure to correct the wrong data input
- There's any adjustment in the computer about the data changing
- There's any language, color design, an interface system which can be easily understanding
- Company can make a documentation of document used
- Time to response the data input will be in short time
- In application system, there will be a save, cancel, and delete.

The problem happened through the input control, first when the input field doesn't have any limit, there will be the operator of data entry will make any mistake when they recording the data and will make any possibility of wrong number in data field. The recommendation is to make a generate to the document and number input field have any limit. Then , the problem happened when the program didn't check the character field (numeric or alphabet), there will be any risk by wrong data input by the employee. For the recommendation, company can make any checking in the character.

Control output in the company, such as:

- Company have any procedure in output checking
- Output interface can be easily understanding
- Company can recheck after the output printed
- Compny have any procedure in authorize the output distributed
- Company have any output received form that approve by the recipient
- Company have a procedure of checking the completeness output
- Printer will placed in the secure located and can be reach by the proper employees
- Application system can produce a proper report

The problem happened in the company are, First the company didn't make any schedule in saving data output, there will be a risk when the output didn't use anymore in the future but the documentation still in the administration. The recommendation is better when the company have any procedur to make a time limit of documentation the output document depends on how long the output will be used. Then, the company didn't have any procedure to ensure how long the output will be used, there will be a risk when the information used by the other unauthorized person.The recommendation beter when the company have any procedure to disposal the output when the living time is end.

5. Conclusion

The conclusion we can take from this analysis are the overall audit system in the company in the general control and application control in information system delivery is good and ther's no potential risk was happened in the company that will impact to the information system delivery.

References

[1] M. J. Abdolmohammadi and S. R. Boss, "Factors associated with IT audits by the internal audit function", in *International Journal of Accounting Information Systems*, vol. 11, no. 3, Sep. 2010, p. 140–151.

[2] N. M. M. A. Malkawi, M. N. Alraja, and T. Alkhayer, "Information Systems Auditing Applied Study at Banks Listed in the Damascus Stock Exchange Syria," in *European Journal of Economics, Finance and Administrative Sciences*, iss. 21, 2010.

[3] B..Yun and Y. Guan, "The Research of IS Auditing Theory System in Information Technology Era," in *Proc. of 2009 International Conference on Management Science and Engineering*, from: http://www.seiofbluemountain.com/upload/product/200910/2009glhy07a7.pdf

[4] Hirth, R. B., "BETTER Internal Audit Leads to BETTER Controls," in *Financial Executive*, vol. 24, iss. 9, Morristown: Nov 2008, pg. 49-51.

[5] H. Keizer, "Utilizing Internal Audit: A CFO's GUIDE," in *Financial Executive*, vol 25, no. 10, Dec. 2009, pp. 46-49.

[6] A. Ortiz, "Internal Controls and IT Audits: Avoiding information security risks in information systems," in ISSA Journal, vol. 6, iss. 2, Feb 2008, pp. 24-26.

[7] C. C. Verschoor, "Swanson on Internal Auditing: Raising The Bar," Book Review, in *Internal Auditing*, vol. 26, iss. 1, Jan/Feb 2011, pp. 46-47.