

# Information Technology Control Evaluation on Sales Module of Pinnacle Software at a Multi-level Marketing Company in Indonesia

Aisyah Indarsari<sup>1</sup> and Lufti Yulian<sup>1</sup>

<sup>1</sup>Faculty of Economics and Business, Universitas Indonesia, Jakarta-Indonesia

**Keywords:** Information technology control, General control, Application control, Multi-level marketing

**Abstract:** Multi-level marketing companies are very dependent on the reliability of information technology used, because with this information technology, multi-level marketing distributors can rely on information relating to the development of their networks that have been built and maintained, and the commission income that has been and will be received. System reliability depends on the quality of the controls applied. Therefore, this study will evaluate the information technology control of Pinnacle software at PT X, a multi-level marketing company in Indonesia, and ensure the calculation of commission income and bonus of PT X's distributors conducted by the Pinnacle software is in accordance with the commitment offered by the company. This research was conducted with primary data collection methods through interviews, observation and testing. The test results state that in general the information technology control of the Pinnacle software in the form of general controls and applications has been done correctly and precisely. The comparison of commission calculation based on Pinnacle results is also in accordance with PT X commission payment scheme policies. Although the Pinnacle network and system security risks have been transferred to the Head Office in the United States as the software license owner, it is recommended that PT X still have written backup plan and contingencies in dealing with disaster conditions and socialized to employees. So that the reliability of Pinnacle PT X software is also supported by its ability to recover faster in the event of a disaster.

## 1 INTRODUCTION

Companies take advantage of the information technology they have as opportunities for growth and competitive advantage against their competitors. Computerized networks, telecommunication systems via satellite, software and hardware that were connected, facilitate the global economy (Douglas, 2002). The process of producing goods and services becomes faster and more effective with the help of information technology systems (Miles, 2001).

But information technology is also vulnerable to the threat of attackers from outside the company and from within the company (Flowerday and von Solms, 2005). The results of Diaz-Gomez's research, et al (2011) stated that the highest threat for information technology crimes originates from within the company. However, Diaz-Gomez further stated that threats from inside and outside the company should give hint to management for

improving security mechanisms. While threats that originally unknown, indicates that the security mechanism is invalid. It also signifies that security policies, procedures and standards are not carried out properly.

The direct selling industry is one of the longest and most traditional forms of sales that has been carried out globally. KPMG's research (2014) stated that the direct selling industry and multi-level marketing in 2012 were successful industries operating in one hundred countries in the world with a market size of 167 billion US dollars globally. The largest market share was in the Asia Pacific region of 44%, followed by countries in North America (20%), South and Central America (20%), European countries (15%) and the rest of African and Middle Eastern countries (0.8%).

In Indonesia, the direct selling and multi-level marketing industries are industries that their value of trade transactions significantly increased over time. According to Djoko Jartanto Komar, Chairperson of

the Indonesian Direct Selling Association (APLI), as quoted from APLI (2018), the value of direct sales and multi-level marketing transactions in Indonesia in 2014 reached IDR 12.6 trillion. The value of transactions in this industry continues to increase, and in 2016 reached IDR 15.75 trillion (Cahyani, 2018).

Multi-level marketing companies are very dependent on the reliability of information technology used, because with this information technology, multi-level marketing distributors can rely on information related to the development of networks that have been built and maintained, as well as revenues in the form of commissions and bonuses that have been or will be obtained. Thus, the level of trust of multi-level marketing distributors towards companies will continue to increase. The problem is as a user, we do not know the reliability of the system used. System reliability depends on the quality of the controls applied. Therefore this study will evaluate the information technology control of Pinnacle software at PT X, a multi-level marketing company in Indonesia.

## 2 THEORETICAL FRAMEWORK

The definition of internal control used in this thesis is the definition conveyed by COSO (1992), which is a process influenced by the board of directors, management, and other organizational personnel, designed to provide adequate guarantees regarding the achievement of several objectives, namely effectiveness and efficiency operations, reliability of financial reporting, and compliance with applicable laws and regulations.

Bae & Ashcroft (2004) stated that traditional controls cannot detect risks arising from adjustments, reengineering processes, software and incompatibilities during the process of implementing Enterprise Resource Planning (ERP). Therefore, information technology control is needed. Information technology control is a separate part of the overall internal control system. Understanding information technology control / IT control according to GTAG (2005) is an internal control process that guarantees information and information services and helps reduce risks associated with the use of technology by organizations.

According to GTAG (2005), information technology controls are generally classified into two categories, which are general control and application control. General control guarantees that all application controls can work effectively, because

effective general controls will reduce identified risks beyond application control.

Chan & Lao (2009) stated in their study that information technology general control (ITGC) is the basis of controls embedded in information technology infrastructure services and applications such as operating systems, databases/ databases and networks, and ensures that they are sufficient enough to provide reasonable guarantees and support for information technology business processes and applications. Arens, et al (2013: 394-398) classify general controls in six categories, including:

1. Administration of the information technology function.  
Some evaluation points that can be used to assess whether the administration of information technology functions of a company have been well controlled, including:
  - (1) The views of the board of directors and senior management about information technology used by the company.
  - (2) Policy of resource allocation provided by the board of directors and senior management for information technology used by the company.
  - (3) The participation of the board of directors and senior management in making core decisions on the use of company information technology.
  - (4) A present of periodic report on the utilization of company information technology from the company's senior management of the information technology (IT) division.
2. Separation of information technology duties.  
Examples of the separation of duties that are ideal for information technology functions of a company according to Arens, et al (2013: 398-399): IT management, both Chief Information Officer (CIO) or Information Technology Manager, Security administrators, System analyst, Programmers, Computer operators, Librarians, Network administrators, Input/output data control personnel.
3. System development.  
Some evaluation points that can be used to assess whether system development of information technology in a company have been well controlled, including:
  - (1) Involvement of IT and non IT staff to make decisions on the company's information technology needs.
  - (2) Implementation of new systems' testing, and good procedures for switching from the old system to the new system.

- (3) Proper system documentation for all new and modified software.
  - (4) Procedure for storing system documentation with storage personnel in an appropriate manner, to ensure that only official software is used.
4. Physical and online security.  
Some evaluation points that can be used to assess whether physical and online security of information technology in a company have been well controlled, including the presence of:
- (1) Physical control of the computer by applying special access codes at the entrance, security cameras and security personnel.
  - (2) Control of room temperature to ensure equipment is functioning properly, and ensure the availability of fire extinguishers to reduce fire risk
  - (3) Restrictions on using online software or downloading unauthorized files using special user IDs and passwords for authorized personnel.
  - (4) A written and monitored security plan
5. Backup and contingency plans.  
Some evaluation points that can be used to assess whether backup and contingency plans of information technology in a company have been well controlled, including the presence of:
- (1) Backup battery or generator to protect the loss of data when the power is off.
  - (2) Backup and contingency plan to deal with more serious disasters, such as data storage outside the city / outsourcing that specializes in secure data storage
  - (3) Backup plan to use alternative hardware that can be used to process company data during the disaster process
  - (4) Copies of software and backup data files in the event of a disaster
6. Hardware control.  
Some evaluation points that can be used to assess whether hardware control of information technology in a company have been well controlled, including the presence of:
- (1) Features on the computer that can detect and report equipment failures.
  - (2) Procedure for handling errors shown by the computer.

According to De Bruijn & Op Het Veld (2008), application control is implemented in an information technology system or ERP and is used every time a transaction goes through the system. In other words, this control is activated and effective for the entire population, where this control usually exists in the regulatory function in information technology systems or ERP. Arens, et al (2013: 394-398) stated

that application control is designed for each software application, and is intended to help companies fulfill six audit objectives related to transactions, namely existence, completeness, accuracy, classification, timing and posting and summarization. Furthermore, Arens et al. classify application control in three categories, namely input control, processing control and output control.

Input control is designed to ensure the information entered into the computer is legal, precise and complete. This is important, because most errors in information technology systems come from data input errors. If the inputted data is wrong, then the information generated (output) will be unreliable. Processing control is intended to prevent and detect errors when transaction data is processed. Output control focuses on detecting errors after the data process is complete.

### 3 RESEARCH METHOD

This research was a case study. This study used primary data collection methods through interviews and observation. The data used as primary data in this study were data or information obtained directly from the informant through an interview process with PT X's IT staff and other staff who use the Pinnacle software at PT X. Observations were made on all related activities with the use of the Pinnacle software at PT X. The Pinnacle software used by the research is the Pinnacle software used at the PT X Office in Jakarta, Indonesia only, so it couldn't reflect the condition of other PT X's group globally. The observation process was also carried out as a tool to verify the truth of the results of the interviews that had been conducted.

The data that obtained from the interview were a general description of business processes, information technology in the form of Pinnacle software used by PT X, information technology controls that have been implemented by PT X during the January-November 2018 period, as well as problems that PT X may have or is facing with the existing information technology control conditions. In addition, observations were made by monitoring the workings of the Pinnacle software from IT staff's computer or other users, starting from the input, process to the output produced, as well as testing the commission and bonus modules on the software. Testing was limited to sales module and calculation of PT X's multi level marketing distributor commission, especially direct income and growing income schemes.

## 4 ANALYSIS

The following were the results of the general control analysis of the Pinnacle software used by PT X in order to evaluate the reliability of the software:

1. Administration of the information technology function.

Directors and senior management are actively involved in making the core decisions of Pinnacle used at PT X. Issues around using Pinnacle can be easily communicated between staff as Pinnacle users and IT staff to directors and senior management. However, based on observations there are no specific periodic reports on the use of Pinnacle from PT X IT staff to the board of directors and senior management. All information and communication related to the use, problems and needs of Pinnacle are delivered verbally and unwritten or specifically documented.

2. Separation of information technology duties.

The position of the Chief Information Officer (CIO) or Information Technology Manager is held by the Head Office in the United States office. And also the role of the security administrator, system analyst, librarian and network administrator were at the Headquarters in the United States office, as they are the Pinnacle software license's owner. The role of PT X is only as user/operator and data input/output control of Pinnacle. The only access that is owned by PT X as a user/operator is to input data and obtain reports on Pinnacle data processing. There is no gap to take unauthorized action or misused of the system's knowledge to commit fraud/gain personal benefits.

3. System development.

Decisions taken by directors and senior management were always carried out based on the needs of staffs as users of Pinnacle. For routine system updates as part of maintenance will be carried out by Head Office's IT staff remotely to the computers of each PT X staff in Indonesia. All email data and Pinnacle input data are stored in the Headquarters database server in the United States. PT X only has a Dynamic Host Configuration Protocol / DHCP server that is used to allocate the IP address (IP address) of all computers in the PT X network. So that PT X has no risk of maintaining or storing the Pinnacle database in the Jakarta office.

4. Physical and online security.

Physical security of Pinnacle had been carried out by installing fingerprint access at the main entrance of the PT X office. This could avoid the risk of irresponsible outsiders entering into the office, or even to access the employee's computer. All computers used by employees also have their own username and password which must be changed every four months. In terms of online security, none of the PT X employees have access to download programs online from the internet, except IT staff as administrators. System or software updates required will be carried out remotely by the IT staff of Headquarters in the United States.

5. Backup and contingency plans.

Facilities related to network security and the ease of use of the Pinnacle software provided by the Head Office in the United States is a form of risk transfer which has been carried out by PT X appropriately. As a user/operator, PT X can focus more on allocating its resources to sales targets and business development. However, PT X does not have a backup and contingency plan for asset protection if it faces a disaster that might occur. In the case of planning procedures to deal with disasters such as fire or earthquake, PT X as a tenant only follows the procedures determined by the building provider.

6. Hardware control.

PT X's Pinnacle supporting hardware has been equipped with error detection, such as a UPS located in the server room that will make warning sound if occurs a sudden loss electricity. Likewise, if the network connection, both the internet connection and the server, is being interrupted, certain icons will appear on the monitor screen of each computer. All employee as Pinnacle user can at any time report the condition of his hardware/computer if indeed there is a problem to PT X's IT staff. IT staff will conduct investigations, trace problems until found causes, and make efforts to solve problems.

The result of the general control evaluations was presented in Table 1.:

Table 1: The result of general control evaluation of PT X's Pinnacle software

No	Type of General Control	Availability		Application	
1	Administration of the information technology function	Yes	No		Mostly Good
2	Separation of information technology duties	Yes		Good	
3	System development	Yes		Good	
4	Physical and online security	Yes		Good	
5	Backup and contingency plans	Yes	No		Mostly Good
6	Hardware control	Yes		Good	

And the following were the results of the application control analysis of the Pinnacle software used by PT X in order to evaluate the reliability of the software:

1. Input control.

Input control of Pinnacle software has been done correctly. This can guarantee and ensure that the information entered into the computer is legal, precise and complete. It is expected that the output produced can also be relied upon. This is based on observations which show that: (1) The input screen has been adequately designed with previously formatted instructions for transaction information, (2) A list of available software selection menus that is easy to understand, (3) The computer performs a validation test against input accuracy, (4) Pinnacle has online-based input control for e-commerce applications where external parties, such as customers and suppliers, carry out the initial part of transaction input, (5) The input error will cause an error message window in Pinnacle, (6) There is a feature of accumulating errors in error files for subsequent follow-up by data input personnel in Pinnacle.

2. Process control.

Based on the results of observation and testing, it showed that the application control in the form of process control has been carried out properly. Tests that have been carried out including validation test, sequence test, reasonableness test, completeness test, limit test, duplicate test and table look up. This can guarantee and ensure that the Pinnacle software used by PT X can prevent, detect and correct process errors. Preventable process errors, known early on and even corrected, can

prevent inaccurate outcomes. So that the reliability of the software can be guaranteed.

3. Output control.

In general, the results of testing the Pinnacle software output control for sales and commission features have been well implemented. This is based on the following observations and tests: (1) Reconciliation of the output produced by Pinnacle to the total number of manual controls has been carried out accordingly, (2) Comparison of examples of transaction outputs with input source documents is appropriate, (3) There are restrictions on access to final results/output that is only for parties who have authorization with user ID and password, (4) Verification of date and processing time that identifies processing data has been running sequentially, (5) Comparison of nominal with funds transferred to the destination account that has been registered and approved previously are in accordance, (6) Comparison of commissions based on the calculation of Pinnacle with the policy/commitment of PT X's commission payment scheme shows compliance.

The result of the application control evaluations was presented in Table 2.:

Table 2: The result of application control evaluation of PT X's Pinnacle software

No	Type of Application Control	Availability		Application	
1	Input control	Yes		Good	
2	Process control	Yes		Good	
3	Output control	Yes		Good	

## 5 RESULTS

Based on the evaluation of information technology control of Pinnacle software used by Pinnacle PT X in the form of general control, it can be concluded that control of Pinnacle software information technology in general has been done and applied properly and correctly.

Recommendations that can be given in line with the results of evaluating the information technology control of Pinnacle software used by PT X include:

(1) At present there are no specific periodic reports on the use of Pinnacle from PT X IT staff to the board of directors and senior management. All information and communication related to the use, problems and needs of Pinnacle are delivered verbally and unwritten or specifically documented. It is better for PT X IT staff to have a periodic reporting format for the use of Pinnacle delivered to directors and senior management. Periodic documentation can be used as a historical documentation of problems and their solutions or development/updates that have been made on Pinnacle. If in the future there are obstacles similar to those that have happened in the past at PT X, then the directors and senior management can look back at the previous report to be used as recommendations and input for their decision making. Directors and senior management can also provide consideration and input for Pinnacle's better performance in the future,

(2) At present PT X does not have a backup and contingency plan for asset protection if it faces a possible disaster. It is advisable for PT X to have a backup and contingency plan procedure for dealing with disasters, which is written and socialized to employees on a regular basis, so that employees understand their respective duties and responsibilities if a disaster occurs at any time. In the backup and contingency plan procedure, PT X should also consider using other alternative hardware if a disaster occurs. So that the recovery process of PT X after a disaster can be faster, and the business can immediately run again.

Based on the evaluation of information technology control of Pinnacle software used by PT X in the form of application control, including testing input, process and output control, it can be concluded that the Pinnacle software is an information technology that has proven its reliability.

## 6 CONCLUSIONS

Evaluating information technology control can be used to make sure whether the information technology that a company had, is reliable. Reliability comes with the control that applicable and conducted correctly. Information technology control can be measured by two aspect: general control and application control. General control evaluation are including: (1) Administration of the information technology function, (2) Separation of information technology duties, (3) System

development, (4) Physical and online security, (5) Backup and contingency plans, (6) Hardware control.

Application control can be tested in three ways, which are input, process, and output control. Input control can be measured by: (1) The input screen has been adequately designed with previously formatted instructions for transaction information, (2) A list of available software selection menus that is easy to understand, (3) The computer performs a validation test against input accuracy, (4) Software has online-based input control for e-commerce applications where external parties, such as customers and suppliers, carry out the initial part of transaction input, (5) Auto-correct procedure that can perform early detection and input error correction, (6) There is a feature of accumulating errors in error files for subsequent follow-up by data input personnel.

Process control can be done by doing some tests like validation test, sequence test, reasonableness test, completeness test, limit test, duplicate test and table look up. The test will make sure that the software used is reliable to prevent, detect and correct process errors. Preventable process errors, known early on and even corrected, can prevent inaccurate outcomes. So that the reliability of the software can be guaranteed.

Output control can be measured by: (1) Reconciliation of the output produced by Pinnacle to the total number of manual controls has been carried out accordingly, (2) Comparison of examples of transaction outputs with input source documents is appropriate, (3) There are restrictions on access to final results/output that is only for parties who have authorization with user ID and password, (4) Verification of date and processing time that identifies processing data has been running sequentially, (5) Comparison of nominal with funds transferred to the destination account that has been registered and approved previously are in accordance.

## REFERENCES

- APLI. (2018). "Perspective Direct Selling Industry". APLI. 21 September 2018. <<https://www.apli.or.id/tag/apli-directselling/>>
- Arens, Alvin A., Randal J. Elder dan Marks S. Beasley. (2013). Fifteenth Edition. "Auditing and Assurance Services: An Integrated Approach". London, UK: Pearson Education

Limited.

- Bae, B. & Ashcroft, P. (2004). "Implementation of ERP systems: accounting and auditing Implications". *Information Systems Control Journal* 5 (4) 43–48.
- Cahyani, Dewi R. (2018). "Transaksi Bisnis MLM Tembus Rp 15,75 Triliun". *Tempo* 21 September 2018. <<https://bisnis.tempo.co/read/1050063/transaksi-bisnis-mlm-tembus-rp-1575-triliun>>
- Chan, W. H. Brenda & Lao, S. Kai. (2009). "A Study of The Business Value of IT General Controls in China". *Journal of Information Technology Management*. Volume XX. Number 4.
- COSO. (1992). "Internal Control Integrated Framework". USA: Committee of Sponsoring Organizations of the Treadway Commission.
- Diaz-Gomez, Pedro A., et al. (2011). "Internal Vs. External Penetrations: A Computer Security Dilemma". In *Proceedings of the 2011 International Conference on Security and Management*. Las Vegas, USA.
- De Bruijn, Ramon & Op het Veld, Maurice. (2008). "Benchmarking IT application controls: A practical guide for SAP".
- Douglas, K. (2002). *Sociological Theory*. Vol. 20, No. 3, 285-305.
- Flowerday, Stephen & von Solms, Rossouw. (2005). "Real-time information integrity = system integrity + data integrity + continuous assurances". *Computers & Security* vol. 24. 604-613.
- GTAG. (2005). "Global technology audit guide: information technology controls". USA: The Institute of Internal Auditors.
- KPMG (2014). *Direct selling: A global industry empowering millions in India*. FICCI.
- Miles, P. (2001). "Globalization – Economic Growth and Development and Development Indicators". Planet Papers.