

Implementation Of The ISO/IEC 27005 In Risk Security Analysis Of Management Information System

Sri Ariyani*, Made Sudarma**

Department of Electrical and Computer Engineering, Udayana University, Jimbaran Campuz.

ABSTRACT

The study conducted and explains about analysis result of Security Management Information System (SMKI) at UPT SAMSAT Denpasar. This analysis has purpose to find out the level of SMKI at UPT SAMSAT Denpasar. Framework to be used in this analysis process is the ISO/IEC 27005. Section that wants to be analyze is the main task and function at the Section of Motor Vehicle Tax (PKB) and Motor Vehicle Mutation Charge (BBNKB) and service process performed, in this case is which is done by the staff in the Section of PKB and BBNKB that includes determining tax, to take data of progressive tax, data slot that involves in it, supporting structure and infrastructure and, of course, the stakeholder who involve in the process. The analysis was performed by implemented the ISO/IEC 27005 framework referring to clause 7 and clause 8. Clause 7 of ISO/IEC 27005 in this analysis was performed to the organization structure, obstacles list that influence the organization, reference list of legislative and regulation that valid to the organization. Whereas clause 8 of ISO/IEC 27005 include asset identification, asset appraisal, impact assessment. Analysis result shows that asset list that has the highest risk rate include the main asset those are: the process of coding selection, determining tax, process of determining the progressive tax ownership status, process of determining the progressive tax ownership order, process to repeat data capture of progressive tax, and supporting asset that cover: staff of determination, staff of progressive data capture. Whereas asset list that has the highest threat level include main asset those are: process of tax determination coding selection, process of progressive tax ownership status determination, process of progressive tax ownership order determination, process to repeat data capture of progressive tax, and supporting asset those are: the staff of determination, staff of progressive data capture.

Keywords: Audit of information system, ISO/IEC 27005, Online SAMSAT

I. INTRODUCTION

International standard organization that handles information security management system (SMKI) is the ISO 27005. ISO/IEC 27005 was prepared by Joint Technical Committee of ISO/IEC JTC 1, information technology, Sub-committee SC 27, security technical TI [1]. The first edition of ISO/IEC 27005 canceled and replaced ISO/IEC TR 13335-3:1998, and ISO/IEC TR 13335-4:2000, which was a technical revision [2]. This standard gives guidance to information security risk management in an organization, supporting, especially, the requirements of Information Security Management System (SMKI) according to ISO/IEC 27001. But, this standard does not supply special methodology for information security risk management [3]. It is up to the organization to determine their approach with risk management depends on, for example, the SMKI scope range, context of risk management, or industrial sector. Some methodologies available can be used in the framework is explained in this standard to apply the requirements of SMKI. This standard is relevant with related manager and staff with management information security risk in an organization and, where, the external side that according and supporting the activity. UPT SAMSAT Denpasar is

one of 9 (nine) UPT of Main SAMSAT Service at Bali Province. UPT SAMSAT Denpasar located at Denpasar, with one Sub UPT located at Renon, SAMSAT Corner at Tiara Dewata and SAMSAT Link at Tohpati [4]. By implementing Online SAMSAT service by Bali Province Government it makes possible for people to pay their motor vehicle tax at SAMSAT Joint Office in all Bali, UPT SAMSAT Denpasar does not only serve people/tax payers who have domicile according to the administration of Denpasar, but all people who wants to pay their motor vehicle tax and doing activity in Denpasar [5]. Transaction that can be served in UPT SAMSAT Denpasar and other Main UPT include: mutation charge, inheritance, enter mutation between *samsat*, lost/damaged Motor Vehicle Lisence, change name, change address, change shape, change plate number, validation of Motor Vehicle Lisence for every year, validation of Motor Vehicle Lisence for 5 years, change vehicle color, change characteristic, change name, mutation to other area, enter mutation between provinces, new vehicle registration, change machine, special vehicle registration [6].

The condition of so many services causes transaction served in UPT SAMSAT Denpasar is also many, which include almost 50% (average of

3,000 transactions) from daily SAMSAT transactions of all Bali. But in the implementation, the service at UPT SAMSAT Denpasar can be said as not maximum. This can be proved by so many problems that came into Helpdesk Section which came from UPT SAMSAT Denpasar or from other UPT due to transaction at UPT SAMSAT Denpasar. The number reaches 75% from total problems that came into the Helpdesk Section where writer performed the task. This matter motivates writer to perform audit regarding the condition of service at UPT SAMSAT Denpasar performed by Revenue Department of Bali Province, especially in the matter of risk management, therefore it is expected that in the future this audit result can give an image to decision makers at UPT SAMSAT Denpasar to find out the risks faced especially regarding to information security and level of the risk influence to the institution. This report will discuss about audit of service performance at UPT SAMSAT Denpasar that refers to ISO/IEC 27005 framework. There were many researches have been carried out related to PKB and BBNKB taxation among others by Eka Purnamawati and NP. Eka Widiastuti that researched about the impact of progressive tax rate imposes at DKI Jakarta Province [7]. Gusti Eryandi, Lizar Alfansi, Benardin researched about the analysis of PKB and BBNKB impose effectiveness in increasing region's original revenue in Bengkulu Province [8]. Gede Pani Esa Dharma and Ketut Alit Suardana researched about the influence of tax payer consciousness, taxation socialization, and service quality to tax payer pursuance [9]. Haula Rosdiana researched about concepting the model of PKB and BBNKB revenue projection [10].

II. LITERATURE REVIEW

A. ISO / IEC TR 1335

The ISO / IEC TR 13335 is used to give guidance, not solution, on information technology security management aspect. People in an organization who are responsible for IT security should be able to adapt with the materials in ISO/IEC TR 13335 standardizations to meet the review of their specific needs. Main purposes of technical report of ISO/IEC TR 13335 are:

1. To define and explain the concepts related to the IT security management,
2. To identify the relation between IT security management and IT management in general,
3. To present some models that can be used to explain the IT security, and
4. To give general guidance about the IT security management.

ISO / IEC TR 13335 is arranged into some sections:[1]

1.Section 1 (ISO / IEC TR 13335-1)

Section 1 gives a description of basic concept and model that is used to describe the IT security management. Section 1 also describes the management and planning aspects. These materials are suitable for managers and those who are responsible for IT security and for people who are responsible to organization security program as a whole.

2.Section 3 (ISO / IEC TR 13335-3)

Section 3 (technique for IT security management) explains about technique of security that is used by the people who involve with the activity of the project's life cycle management, the review that include planning, designing, implementation, testing, acquisition, or operational.

3.Section 4 (ISO / IEC TR 13335-4)

Section 4 (protection selection) gives guidance for protection selection, and how this matter can be supported by the usage of basic model and control. Section 4 also explains about how to complete security technique explained in Section 3, and how the evaluation of additional methods that can be used for security selection.

4.Section 5 of ISO / IEC TR 13335-5

Section 5 (guidance management about network security) gives guidance regarding to network and communication, the review of those who are responsible upon the IT security management. This guidance supports identification and related communication factor analysis that should be reckoned to build the requirement of network security.

B. ISO IEC 27005

This standard includes the description of information security risk management process and its activities. Background information is given in Clause 5. General description of information security risk management process is given in Clause 6. All activities of information security risk management as presented in clause 6 will be explained in the following clauses: context determination in Clause 7, risk evaluation in Clause 8, risk treatment in Clause 9, risk acceptance in Clause 10, risk communication in Clause 11, risk monitoring and reviewing in Clause 12v[3]. All risk management activities presented in Clause 7 to Clause 12 are arranged as: Input (*Identifying any information needed to perform an activity*), Action (*Explaining activity*), Manual of Implementation (*Giving manual to perform action*), Output (*Identifying any information obtained after performing activity*). Some of these manuals might

not be suitable in all cases and other ways therefore performing action might be more proper.

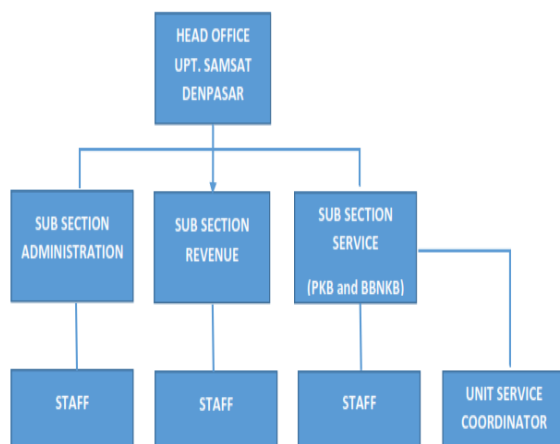
III. RESEARCH METHOD

- Risk analysis was performed at UPT SAMSAT Denpasar. Framework to be used is the ISO/IEC 270005, clause 7 about context determination, and clause 8 about risk evaluation.
- Analysis focus is to the main task and function at Section of Motor Vehicle Tax (PKB) and Motor Vehicle Mutation Charge (BBNKB) and the process of service performed, in this case is performed by the staff of Section of PKB and BBNKB that covers the process of tax determination, progressive tax data capture, data slot involved in it, supporting structure and infrastructure and of course the stakeholders who involved in the process.
- By refer to clause 7 ISO/IEC 27005, the analysis in this research was performed to the organization structure, obstacles list that influence the organization, reference list of legislative and regulation that valid to the organization. Whereas clause 8 of ISO/IEC 27005 that covers the asset identification, asset appraisal, impact evaluation [3].

IV. RESULT AND DISCUSSION

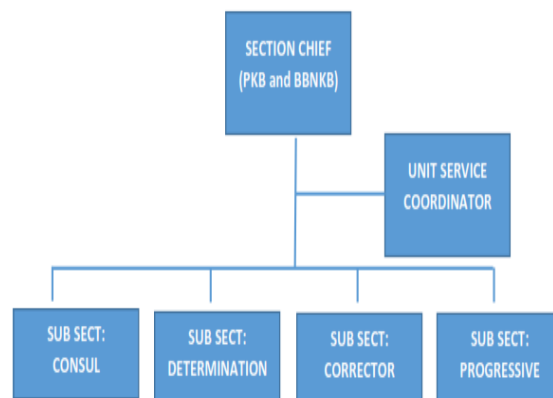
A. Organization Structure

Generally the organization structure of UPT SAMSAT Denpasar lead by a chief of UPT, and assisted by three sub sections those are the sub sections of administrative, acceptance of other revenues, PKB and BBNKB service, as shows in the following picture 1:



Picture 1. Organization structure

In this research the analysis process was done only to sub sections that performing main task and function service, as shows in the following picture 2:



Picture 2. Organization structure of sub sections

B. List of Obstacles that influence the Service Process at PKB and PNKB in UPT SAMSAT Denpasar

Table 1. Obstacles List

OBSTACLES LIST	
No	Obstacles Description
1.	<p>Progressive data capture</p> <ul style="list-style-type: none"> a. Mistake in progressive determination b. Determination of ownership order c. Report on sold vehicle d. Repeat data capture of progressive e. Late application respond especially for progressive data capture f. Mistake in the determination of ownership status g. Lack of carefulness in checking supporting files
2.	<p>Determination and Re-determination</p> <ul style="list-style-type: none"> a. Mistake in determination process b. Mistake in coding selection c. Parameters checking in determining tax amount d. Implementation of tax edit process e. Poor determination manual administration (supplement) f. User login that is usually shared together g. Process of SKPD withdrawal when payment cancellation occur h. Determination process that is performed outside the service time i. Staff's carefulness in checking data from the registration j. Comprehension of determination process by the staff for certain transactions
3.	<p>Correction and corrector</p> <ul style="list-style-type: none"> Corrector's carefulness in performing task
4.	<p>Other</p> <ul style="list-style-type: none"> a. Networks that sometimes discontinues that cause slow moving of application respond and sometimes it has to be reloaded b. UPS that does not function/still damage c. Printer that often damage and no backup d. Service performing for internal staff e. There is no standardization in the service f. Qualification of the staffs and the selection of their position g. There is no SOP that arrange the SAMSAT process in a whole

Generally the obstacles in this analysis process are grouped into two groups those are the obstacles from UPT Internal and obstacles from UPT External. The obstacles from UPT internal are described in the table 1. Moreover the list of external obstacles can be seen in the following table 2:

Table 2. External Obstacles

No.	OBSTACLES LIST	
	UPT External Obstacles	Obstacles Description
1.	Progressive Data Capture	a. Data capture that is performed by proxy b. Data capture that is not valid c. Tax payer who performs repeat data capture
2.	Determination and Re-determination	a. Usage of different application by the police department b. Registration data that is not valid c. Double registration d. Lack of filtering at interface application e. Mistake in transaction mapping f. Registration which is carried out outside the service time g. Mistake in the selection of registration transaction h. Process of transaction cancellation by cashier i. Service to service bureau
3.	Other	a. Network connection b. Application improvement by third party

C. Legislative Reference

Like other government institutions, UPT SAMSAT Denpasar also has legal basic to be a basic for service operational. The list of legislative reference and valid regulations are as shown in the following table 3:

Table 3. Legislative and Valid Regulations

No.	List of Legislative Reference and Valid Regulations to UPT Samsat Denpasar
1.	Bali Province Regulation No.1 Year 2011 About Local Tax.
2.	Regulation of Governor of Bali No.40 Year 2011 about Instruction of the Implementation of Bali Province Regulation No.1 Year 2011 about Local Tax.
3.	Regulation of Governor of Bali No.25 Year 2014 about Basic to Impose the PKB and BBNKB.
4.	Decision of Kadispenda No.973/1072/Dispenda, dated 15 th February 2013 about Instruction of the Implementation Technical to Impose PKB, BBNKB, and Surface Water Tax in Bali Province
5.	Standard Operational Procedure (SOP) of Imposing Progressive Tax for Motor Vehicle To Revenue Department of Bali Province No.973/4494/Pajak/Dispenda dated 2 nd May 2014.

D. List of Asset

In this analysis assets are grouped into two important sections, those are the main asset and supporting asset. List of main asset are shown in the following table 4:

Table 4. Main Asset

No.	List of UPT SAMSAT Denpasar's Asset	
	Main Asset	Description of Asset
1.	Process of Progressive Data Capture	a. Process of ownership order selection b. Process of ownership status determination c. Process to repeat data capture
2.	Supporting Information of progressive data capture	Information of demography data
3.	Process of determination	a. Process of selection/determination of motor coding b. Process of tax audit
4.	Process of Re-determination	
5.	Supporting Information of determination and re-determination	a. Information of transaction data b. Information of payment data c. Information of Master data d. Information of Blockade and Potential e. Information of Mutation Data

Whereas the list of supporting assets is include in the following table 5:

Table 5. List of supporting assets

No.	List of UPT SAMSAT Denpasar's Asset	
	Supporting Assets	Description of Assets
1.	Hardware	a. 18 Personal Computers HP Pro 2000 MT at the service section. b. 12 Personal Computers HP Pro 2000 MT at progressive data capture section with specification: Pentium E5400 (2.7 GHz, 2 MB L2 cache, 800 MHz FSB), 1GB DDR3, 320GB HDD SATA, DVD±RW, Audio, GbE NIC, VGA Intel GMA 4500 256MB (shared), HP USB Standard Keyboard & Optical Mouse, Monitor 15, Win XP Pro. c. 10 Printers of Epson LQ 2170/2180. d. 10 Printers of Laserjet HP 1100. e. UPS Vektor Ablerec.
2.	Software	a. Operational System: Windows XP Pro. b. Office 2007 (not all computers).
3.	Software	a. Operational System of windows XP Professional. b. Microsoft Office 2007.
4.	Network	Computer network is connected to local network of dispenda of Bali Province in the form of local area network.
5.	Business application	a. Online Application of client I-SAMSAT b. Reporting application c. Application of revenue monitoring
6.	Stackholder	a. Chief of PKB and BBNKB service section b. Consul/administrator of UPT c. Staff of determination d. Staff of SPPKB printing e. Corrector staff f. Coding staff g. SKPD printing h. Staff of progressive data capture

E. Asset Appraisal

Asset appraisal was performed by using scale of 0 to 4, where 0 is asset with the lowest value and 4 is asset with the highest value to the organization. Valuation for assets with analysis result performed is shown in the following table 6:

Table 6. List of Valuation of Assets

Asset	Asset's value	Possibility to occur	Exploitation facility	Asset's risk size
Process of progressive data capture	3	Medium	Medium	5
Process of ownership order selection	3	High	Medium	6
Process of ownership status determination	3	High	Medium	6
Process to repeat data capture	3	High	Medium	6
Information of demography data	2	Low	Low	2
Determination Process	4	Medium	Medium	6
Process of coding selection	4	High	Medium	7
Process of tax edit	3	Medium	Low	4
Process of re-determination	4	Medium	Medium	6
Information of transaction data	3	Low	Low	3
Information of payment data	4	Low	Low	4
Information of Master data	4	Low	Low	4
Information of blockade data and potential	2	Low	Low	2
Information of mutation data	1	Low	Low	1
Correction of determination	2	Medium	High	5
Hardware	2	Medium	Low	3
Software	1	Low	Low	1
Network	2	Medium	Low	3
Application	3	Medium	Low	4
Chief of PKB Section/Decision Maker	3	Low	Low	3
Consul staff	3	Medium	Low	4
Determination staff	3	High	Medium	6
SPPKB printing staff	0	Low	Low	0
Corrector staff	2	High	Low	4
Coding staff	1	Low	Low	1
Staff for SKPD printing	0	Low	Low	0
Staff of SAMSAT's Information	0	Low	Low	0
Staff of progressive data capture	3	High	Medium	6
Staff of progressive Information	0	Low	Low	0

F. Valuation of Asset's Threat

Valuation of risk size for each threat was obtained from the multiplication result of consequences value and possibility value of threat that might occur, which are put in order according to risk size value. And data to be used in the determination of valuation is 1 to 5. For each threat exist in the service performance, the analysis result

that has been performed by the writer for every threat is shown in the following table 7:

Table 7. Value of Asset's Threat

Threat	Consequence Value	Threat Possibility	Risk Size	Order of Risk
(a)	(b)	(c)	(d)	(e)
Fire	5	1	5	7
Flood	5	1	5	7
Operational's waste/trash	3	1	3	9
Lightning	4	1	4	8
Water sprinkling	4	2	8	5
Earthquake	5	1	5	7
Disturbance of animals	3	2	6	6
Electric blackout	4	2	8	5
AC down	2	1	2	10
Disconnected network connection	5	1	5	7
Cannot connect application	5	3	15	2
Virus	3	2	6	6
invalid registration data	5	8	20	1
Registration that is not according to transaction	5	3	15	2
Not accorded transaction mapping	5	2	10	4
Not accorded ownership order data	5	4	20	1
Cancellation of transaction by cashier	5	2	10	4
Old registration that has not been removed	5	3	15	2
Registration data that is not filtered	5	2	10	4
Progressive data capture by proxy	5	4	20	1
Report on sold vehicle	5	3	15	2
Repeat progressive data capture	5	3	15	2
Application Server down	5	1	5	7
Database Server down	5	3	15	2
Replication does not running	3	2	6	6
Equipments damage	4	1	4	8
Mistake in determination	5	3	15	2
Mistake in coding selection	5	4	20	1
Tax edit	5	3	15	2
Determination outside service time	4	1	4	8
Mistake in searching progressive data	4	2	8	5
Mistake in determination of ownership order	5	4	20	1
Repeat progressive data capture	5	3	15	2
Printer broken	4	3	12	3
PC broken	5	2	10	4
UPS broken	5	1	5	7
Router, hub, switch broken	5	1	5	7

G. Possibility and Ratio Value

Final step from this analysis process is to find asset's value and possibility value to obtain asset's value and risk possibility which furthermore to be called as system's risk. From analysis result performed by the writer, the valuation result for system's risk is described on the following table 8:

Table 8. Asset's value and Risk Possibility

Asset	Asset's value	Threat Possibility	Level of Susceptibility	Possibility Value	Asset's value and Risk Possibility
Process of progressive data capture	3	Medium	Medium	2	5
Process of ownership order selection	3	High	Medium	3	6
Process of ownership status determination	3	High	Medium	3	6
Process to repeat data capture	3	High	Medium	3	6
Information of demography data	2	Low	Low	0	2
Process of determination	4	Medium	Medium	2	6
Process of coding selection	4	High	Medium	3	7
Process of tax edit	3	Medium	Low	1	4
Process to re-determination	4	Medium	Medium	2	6
Information of transaction data	3	Low	Low	0	3
Information of payment data	4	Low	Low	0	4
Information of Master data	4	Low	Low	0	4
Information of blockade data and potential	2	Low	Low	0	2
Information of invitation data	1	Low	Low	0	1
Correction of determination	2	Medium	High	3	5
Hardware	2	Medium	Low	1	3
Software	1	Low	Low	0	1
Network	2	Medium	Low	1	3
Application	3	Medium	Low	1	4
Chief of PKB Section/Decision Maker	3	Low	Low	0	3
Consul staff	3	Medium	Low	1	4
Determination staff	3	High	Medium	3	6
SPPKB Printing staff	0	Low	Low	0	0
Corrector staff	2	High	Low	2	4
Coding staff	1	Low	Low	0	1
Staff for SKPD printing	0	Low	Low	0	0
Staff of SAMSAT's Information	0	Low	Low	0	0
Staff of progressive data capture	3	High	Medium	3	6
Staff of progressive Information	0	Low	Low	0	0

V. CONCLUSION

From analysis and performed by the writer to asset, asset's risk, threat and system's risk to the service performance it can be mapped the assets and threats that are most risky, those are:

a. Asset

After analysis was performed, assets to the service performance that the most risky are:

- **Main asset:**

1. Process of coding selection of tax determination.
2. Process of progressive tax ownership status determination.
3. Process of progressive tax ownership order determination.
4. Process to repeat data capture of progressive tax.

- **Supporting asset:**

1. Staff of determination.
2. Staff of progressive data capture.

b. Threat

Whereas main threat in the service performance, the analysis result performed by the writer which have the highest risk size are:

1. Not valid input of registration data.
2. Process of progressive data capture by proxy.
3. Mistake in determination of coding selection.
4. Mistake in determining vehicle ownership order.

c. System's risk

After comparing between available assets, threats, and susceptibility level it will obtained main system's risk, those are:

1. Process of coding selection at the time of tax determination.
2. Process of progressive tax ownership status determination.
3. Process of progressive tax ownership order determination.
4. Process to repeat data capture of progressive tax.

The whole processes are the main process that was performed by UPT SAMSAT Denpasar which really determines the amount of tax that should be paid by tax payer. Therefore, those processes mentioned above should be ensured to be worked properly in order of main function and to perform the imposing of Motor Vehicle Tax. From audit result described, the writer recommends some matters that might be able to be done in the future to reduce and even to remove the available main risks in the service performance among others:

- **Automatization of coding selection**

Coding selection for determination performed recently is still manually by carrying out searching to the available coding table. This is, of

course, risky in making mistake in coding selection especially for the similar type of vehicle. Not to mention the high tax payer volume that often sacrificing carefulness to smooth the service process. Therefore, we recommend that the coding selection was performed automatically by the system by inputting manual parameters that during these times were performed by the staffs into the system.

– **Application of strict rules in the implementation of progressive data capture.**

In performing progressive data capture, the tax payers often convey not accorded/valid data to avoid the imposing of progressive tax. Moreover, it's often that the progressive tax data capture is performed by proxy that is to service bureau or other people, so the data conveyed often different with the fact. Therefore, the writer has recommendation to apply stricter rules regarding the data capture by proxy and imposing sanction for tax payers who are intended to convey data of progressive data capture that are not accorded in order to avoid tax.

– **Arrangement by system for the limit to repeat data capture.**

Effect from what was carried out by tax payers in point 2 was the repeating of progressive data capture. After paying tax for their vehicle, the tax payers will perform repeating data capture to re-adjust their vehicle's data, so when they have to pay tax for their other vehicle they will not be in problem. Indeed, the available SOP makes it possible, but it is not being used properly. For that purpose the writer has recommendation to lock it systematically so that the data captured that has been done cannot be updated again and to be blockade. The update can only be performed by certain condition.

ACKNOWLEDGEMENTS

The appreciation is awarded to all the colleagues who have given a lot of help both in discussion of ideas until the trial implementation stage of the study. Not forgotten also the appreciation is delivered to the UPT SAMSAT Denpasar and Department of Electrical and Computer Engineering, Udayana University which has supported in lending the laboratory equipments in this research.

REFERENCES

- [1]. I. S. O. Iec, "International Standard ISO/IEC TR 13335," vol. 2004, 2004.
- [2]. British Standard. BSI "International Standard- ISO IEC 27005"2008.
- [3]. I.S.O. Iec, "International Standard ISO / IEC techniques – Information security risk," vol. 2008, 2008.

- [4]. Gubernur Bali"Perda Bali Nomor 1 Tahun 2011 tentang Pajak Daerah," 2011.
- [5]. Gubernur Bali,"Pergub Bali No 33Tahun 2010 tetang dasar pengenaan PNKB."2010.
- [6]. Gubernur Bali," Pergub Bali No 40 Tahun 2011 tentang Petunjuk Pelaksanaan Perda Bali No 1 Tahun 2011 tentang Pajak Daerah."2011.
- [7]. Eka Ermawati, NP. E. Widiastuti,"Dampak Pengenaan Tarif Pajak Progresif PKB di Provinsi DKI Jakarta" 2012.
- [8]. JEEPP, "Analisis Efektivitas Pemungutan PKB dan BNKB dalam Meningkatkan PAD di Provinsi Bengkulu" Vo. 4, No. 2, 2011.
- [9]. E-Jurnal Akuntansi UNUD, "Pengaruh Kesadaran Wajib Pajak, Sosialisasi Perpajakan, Kualitas Pelayanan pada Kepatuhan Wajib Pajak" vol. 1, pp. 340–353, 2014.
- [10]. H. Rosdiana, "Menggagas Model Proyeksi Penerimaan PKB dan BBNKB," vol. 16, pp. 147–159, 2009.