UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

A Conceptual Framework of Information Security Database Audit and Assessment

Muneeb-ul-Hasan[1], Siti Hajar Othman[2] & Marina Md Arshad[3]
School of Computing, Faculty of Engineering
Universiti Teknologi Malaysia
81310 UTM Johor Bahru, Johor, Malaysia
Email: [1]muneebhasan_parco@live.com, [2]hajar@utm.my, [3]marinama@utm.my

Submitted: 12/06/2018. Revised edition: 26/06/2018. Accepted: 16/07/2018. Published online: 30/05/2019
DOI: https://doi.org/10.11113/ijic.v9n1.206

***Abstract*—Today, databases are one of the most important things in the IT world and organizations globally are gradually moving their traditional IT setup to database model to gain the benefits of securing the data and providing easy access and elasticity to IT services. With database security, the IT service roles within an organization become integrated hence giving the overall IT operating model a more structured layout. Such objective however can only be materialized when proper planning and implementation of database system which include a stringent set of checks and audit processes are put in place. The goal of database auditing is central towards determining if the services engaged and its maintainers are meeting certain legal requirements in terms of protecting customers data and also meeting organization standards in terms of successfully securing data assets against various security threats. Therefore, this paper explores the factors influencing security audit quality by collecting data using structured group discussion.**

***Keywords*—Information Security, Audit, Database Audit, Audit Quality**

I. INTRODUCTION

In the area of information security, the traditional database mechanism systems such as data encryption and access control are basically useless because a trusted employee can have or can easily obtain the right credentials to the data that is stored in that database. To add to this, more enterprise is getting the databases access, such as HR manager, database administrators, application developers and even software engineers. If an enterprise has not done auditing or monitoring of their databases, then their assets are at very high risk [17].

There have been many numbers of proposed solutions for database security, for example, Vanhor [17] states that embedding a system to monitor, and audit databases makes it easier to implement security policies in organizations. Using a database audit can be very helpful in protecting the transaction logs in the database system. However, storing these logs may cause some serious storage and performance problems.

Information security database audit is part of an investigation for auditing and monitoring policies of the organization that is being audited. The purpose of the database audit system is to ensure that every access to the database is recorded immediately and more effectively, and the detailed analysis of the system record is generated, so that the database system can use the five elements to record every incident – when, who, where, what, how [18].

Information Security database assessment is a systemic technical assessment to measure how the security policy is employed by the organizations. It is part of the on-going process of defining and maintaining effective security policies. Together with database audit, they should not only secure the database but also the organization itself so that the organization can perform tasks risk free.

Thus, the objectives of this research are to: i) to investigate factors which effecting the security audit and assessment quality for database audit domain, ii) to propose a conceptual information security framework for database audit and assessment and iii) to evaluate the proposed database audit and assessment conceptual framework by using of the expert review and the validation against other models method.

II. Literature Review

In this section, a quantitative review of database security audit frameworks has been revisited and presented. Database is behind every system that affects almost every aspects of our lives such as our bank accounts, phone records, medical records, employment records. Almost everything is maintained by a modern database management system. If the database system that has significant and sensitive information about our lives is not secured, then the potential impact in our lives and even our broader society, can produce devastating results.

The security of the database system can be elevated with the implementation of user identification, authentication, access control and other measures. But the main problem is that the database is far from secure because these implementations and measures are not capable of monitoring and logging database activities, which can be helpful when an audit is done on a system.

The only solution which we have to this problem is implementing database auditing. Database auditing involves observing a database in order to monitor database users. Security and data centre teams must be sharp enough to implement and enforce a set of best practices to address the insider threats. IT architects must then bolster the policies by using database auditing rather than other security features that has been built into other major database platforms [10].

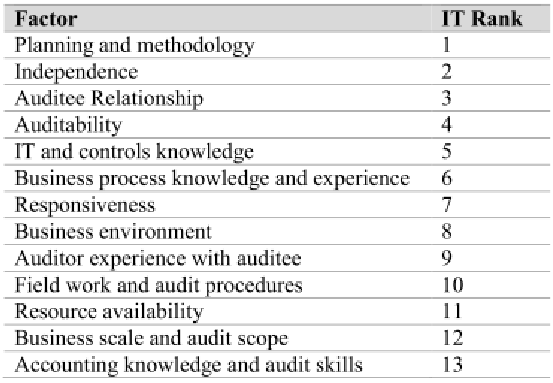
A. IT Audit and the Analysis of Attributes that Impact IT Audit Quality

One very obvious purpose of IT audits is to provide management with assurance that a system or automated process is meeting its objectives. Stoel et. al. [16] had deliberated in detail the importance of IT audit and the IT audit quality. According to their studies, IT audits are widely used internally by organisations to examine the operations effectiveness, controls, and security of critical systems, which will be used to identify opportunities for improvement or areas of weakness. The increased demand for IT audit services emphasizes the importance of performing these services in the most efficient and effective manner.

Furthermore, the attention towards IT audit has risen due to the following two reasons: 1) increased spending and dependence on IT for business operations, and 2) new legislation and professional requirements related to the audit of these operations. IT audits may serve various objectives and multiple parties within an organization and therefore there may be different definitions of IT audit quality. These definitions may include ideas such as impact of effectiveness and completeness related to different standards of efficiency and cost. Specifically, the focus may be on managements' control and responsibilities over computer-based information assets and processes. In these cases, specific standards developed by groups such as ISO, PCAOB, or AICPA may assist in defining certain IT audit quality. Organisation must make appropriate decisions regarding the scope, resources (e.g. personnel or computer-automated audit tools), tasks or activities to be performed, methods and techniques, and other inputs to the IT audit process. Management's decisions regarding specific resources to deploy for a specific IT audit should attempt to maximize the overall audit quality and minimize the cost as related to their specific IT objectives. This also requires a consideration of other attributes that might impact the performance and outcome of the IT audit, but over which they have no or little control. These attributes might include the availability of key auditee personnel, the infrastructure or architecture on which a system is running, or the organizational structure of a business unit being audited.

Due to the above, [16] did a study on factors affecting IT audit quality in which factor analysis was performed unto a series of factors deriving from multiple previous literatures. These factors were then evaluated in terms of their relative importance. Based on the results of the factor analysis and the scores for these factors, 13 factors related to IT audit quality were refined and perceived as the most important IT audit factors on IT audit quality, as shown in Table 1.

TABLE 1. Overall perceived importance of IT audit factors on Audit Quality



Factor	IT Rank
Planning and methodology	1
Independence	2
Auditee Relationship	3
Auditability	4
IT and controls knowledge	5
Business process knowledge and experience	6
Responsiveness	7
Business environment	8
Auditor experience with auditee	9
Field work and audit procedures	10
Resource availability	11
Business scale and audit scope	12
Accounting knowledge and audit skills	13

1) Information Security Frameworks

Cyber security is a complex, ever evolving problem space and a broad, non-technical view is adopted in proposing an information security framework. Present security dilemmas include the porous nature of information security as propriety software is continually upgraded; the proliferation in malware and the sophistication of malware production and management; walled internet communities and mistrust between and among such communities; and the reactive nature of cyber security protection [5].

The Oxford Dictionary (1983) defines a framework as a structure upon or into which contents can be put and further relates it to thoughts that are directed for a purpose. The Information Security Culture Framework proposed in this paper provides organisations with an understanding of how to establish an information security culture to minimise the risks posed by employee behaviour regarding the use of information assets [1].

The Information Security Culture Framework is constructed by systematically considering the various fields of knowledge that affect this type of culture. Various research indicates that it is part of the overall organisational culture that develops based on organisational behaviour exhibited by employees. Organisational behaviour is therefore considered, as are the information security components that must be considered in the implementation of information security. The interaction between these fields of knowledge is illustrated in the following paragraphs and enables the construction of the Information Security Culture Framework [1, 2].

a) COBIT Framework

While a range of frameworks, standards and documents related to the control of IT exist, the primary focus of COBIT is on aligning the use of IT with organizational goals. COBIT is a comprehensive framework of 34 control objectives that has been developed from “41 international source documents” and validated internationally to help balance IT risk against investment in IT controls. The control objectives have been organized into a hierarchy of processes and domains that are designed to help bring about the alignment of business and IT objectives, by identifying the requirements for IT resources and information associated with 318 detailed control objectives. IT processes are grouped into four domains: planning and organization, acquisition and implementation, delivery and support and monitoring. As the framework considers all aspects of information and its supporting IT, management can use COBIT to help provide an appropriate control system for IT [6].

COBIT's underlying conceptual model asserts that to satisfy business requirements, information must meet seven criteria: (1) Effectiveness, (2) Efficiency, (3) Confidentiality, (4) Integrity, (5) Availability, (6) Compliance, (7) and Reliability (Appendix B provides detailed descriptions for each criterion as presented in COBIT 4.0). The conceptual model relates each COBIT process to the information criteria that the process affects, and therefore, should provide an auditor with means of directly assessing specific controls for their effect on the quality of information, whether the audit is operational, compliance, or financial in nature. Furthermore, there are clear linkages between the COBIT information criteria and COSO's objectives related to the effectiveness and efficiency of operations, compliance with laws and regulations, and reliability of information.

Achieving the COBIT information criteria, therefore, has important implications for financial statement assertions as well as broader implications for the efficiency and effectiveness of operations [3].

b) COSO Framework

COSO published the first formalized guidelines for internal controls, Internal Control Integrated Framework, in 1992. This publication established a common definition for internal control and a framework against which organizations can assess and improve their control systems. In 1994, COSO’s work was endorsed by the head of the General Accounting Office (GAO) of the U.S. Congress. These voluntary industry guidelines were intended to help public companies become self-regulating and thus avoid the need for governmental regulation of the accounting and auditing industries [5].

Internal control is a process, affected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

The following are key concepts of internal control according to COSO:

- Internal control is a process. It is a means to an end, not an end in itself.
- Internal control is affected by people. It’s not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only reasonable assurance, not absolute assurance, to an entity’s management and board.
- Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.

The Internal Control Integrated Framework publication introduced what is now a well-known graphic, the COSO cube [7] as shown in Figure 1.

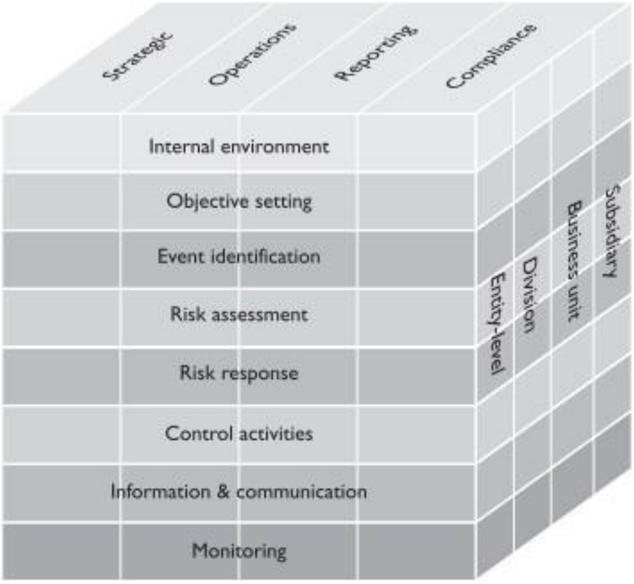


Fig. 2. COSO expanded cube

2) Preparation Phase

Everything that is conducted in advance by related parties such as audit manager, auditor, and client in order to ensure that the audit complies with client's requirements and objectives are done during the audit preparation phases. In the preparation stage of an audit process, it usually begins with the reason to carry out the audit. Auditor begin to analyse all the requirements and objective requested by the clients. This phase consists of activities such as commissioning the auditing group and creating the audit project plan or blueprint before the actual implementation of audit [12].

3) Performance Phase

Russell [13] states that the performance phases of an audit is commonly defined as the fieldwork. Performance phase is the information collecting stages which covers the time period from arrival at the audit location until the exit meeting. Some of the on-site auditing activities includes meeting with the audit team member, communicating with team members and auditee, understanding the fundamental of the process and system controls, analysing whether these controls work through verification, and on-site information gathering such as firewall, server, network topology, router devices, existing policy, and others.

After that starts the groundwork for audit team member to conducts the audit process such as penetration test on organization parameters, reviewing or enhancing the existing IT policy, analysing the strength of access control from both technical based and administrative based. The auditing process can be done either internally or externally. Lastly, they will analyse the audit results to prepare for the next phases of audit which is conclusion phase [12, 13].

4) Conclusion Phase

The objective of the audit report is to address the outcomes of the audit investigation. The report ought to offer accurate and clean effective information as a useful management resource in addressing vital organizational problems. Activities executed in this phase are sharing audit results, writing audit results, and dealing with resistance to audit recommendations.

After that, an audit closure and follow-up will be carried out to further correct any mistakes in the audit report. Lastly, ISO Standard 19011, clause 6.6 states that "The audit is completed when all the planned audit activities have been carried out, or otherwise agreed with the audit client." Clause 6.7 of ISO Standard 19011 continues by stating that verification of follow-up actions may be part of a subsequent audit as it is part of building an ongoing audit program. In the end, the audit procedure is considered ceased when the report has been issued by the lead auditor or after evaluation and follow-up actions have been completed [12].

5) Information Assets

Information assets are important in the field of IT. Basically, information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognizable and plausible value, risk, content materials and life cycles. That is why the assets are the most important part of any organization database and because of the sensitive information they possess, these assets or information needs to be secured [2].

The basic concept here is to make manageable portions by making groups of individual pieces of information. If one had to assess a huge amount of document, database and pieces of record, then he will have an impossible task of combing through millions of items. If the items are grouped at a level that will match the objectives, then one can make the task achievable [2].

Information assets should be identified according to the description above and the extent of granularity that is required to meet the goals. An information asset is defined at a stage of detail that allows its constituent components to be managed usefully as a single unit [11].

III. INFORMATION SECURITY DATABASE AUDIT AND ASSESSMENT FRAMEWORK

In this section we outlined the design and development of the audit process as illustrated by the conceptual framework.

A. Information Security Database Audit and Assessment (ISDAA) Framework

Illustrated in Figure 2 is the proposed framework which is based on the previous studies discussed in the literature review. Auditing of a database must be done on a periodic basis. There are three main reasons to this. Firstly, periodical assessment can mitigate the risks introduced by the database system. Secondly, efficiency of controls relating to the database can be evaluated and finally, the audit review can help to continually improve internal process, procedures and tools thus the overall effectiveness and efficiency of database system implemented. However, there was no dependent variable defined for this study because participants were required to focus more on the audit processes that influence security audit quality. Therefore, the security audit quality was qualified as the evident outcome of the proposed model as shown in Figure 2. The audit quality signifies the construct to measure the success of the database security audit process by assuming that each factor that contributes to the quality have a direct relationship with it.

The following steps are employed for the ISDAA framework:

1) Oracle Database Control

Database is a collection of all the related data which is organized in such a manner that it can be accessed by multiple users for validation purposes. Database controls are designed to ensure that all the security, integrity, accountability of the database is well controlled. Information management has many problems. The key to finding these problems is database servers. In general, a server involves some multiuser environment and management of large amount of data so that the users can control the data easily. All this of these things will be accomplished if the delivery is in high performance.

Oracle database system was designed as the first database for different enterprises so that the cost-effective way should be flexible enough to manage different information and applications. Enterprise grid is an architecture in which each new unit is rapidly provisioned from the components. For the capacity to be added or relocated from the resource components there will be no need of weak loads. The database has two types of structures:

i. Logical Structures
ii. Physical Structures.

Because both the structures are different and separate, the physical storage of data can be managed without interfering with the logical storage patterns. The oracle database will be the focused database to audit in UTM CICT. There are 2 kinds of databases in CICT:

i. Oracle Database
ii. SQL Database

2) SQL (DML)

DML is abbreviation of Data Manipulation Language. It is used to retrieve, store, modify, delete, insert and update data in database. The statements will be created once the audit of the database is done. Oracle supports three different kinds of audits enabled via various syntax of the SQL command Audit:

i. Statement
ii. Privilege
iii. Object

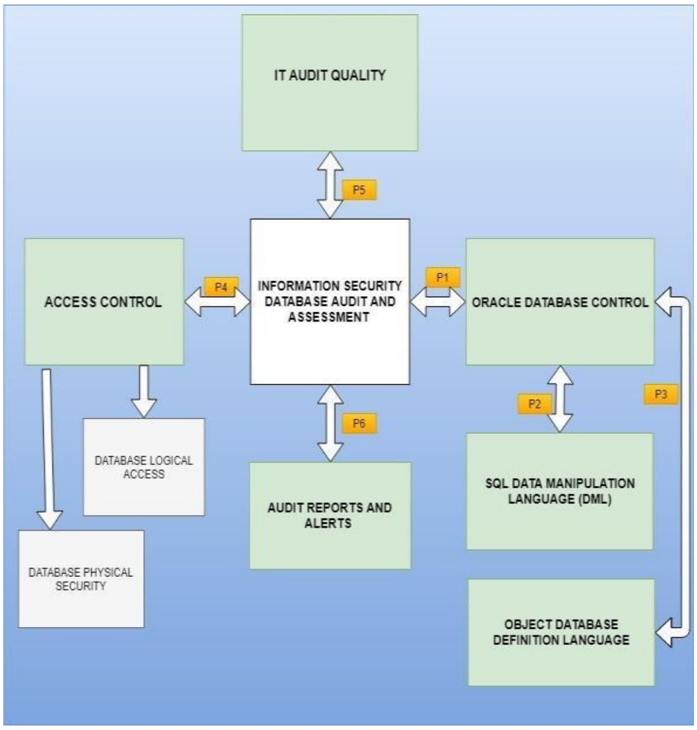

IT AUDIT QUALITY
P5
ACCESS CONTROL
P4
INFORMATION SECURITY DATABASE AUDIT AND ASSESSMENT
P1
ORACLE DATABASE CONTROL
P2
P3
P6
DATABASE LOGICAL ACCESS
DATABASE PHYSICAL SECURITY
AUDIT REPORTS AND ALERTS
SQL DATA MANIPULATION LANGUAGE (DML)
OBJECT DATABASE DEFINITION LANGUAGE

Fig. 2. Information Security Database Audit and Assessment Framework

3) Object (DDL)

A data definition language or data description language (DDL) is a syntax similar to a computer programming language for defining data structures, especially database schemes. In the auditing phase of the database, this command comes under the standard oracle auditing and is used to create and alter the objects.

The access and usage of some objects can be audited by allowing object auditing process. The statement/privilege audit is a very important part of this process which can be modified enough to audit some specific users. Object auditing process has many users, but it has only a limited of object to be audited.

The AUDIT ANY privilege is required to have an object audit which should be general in all aspects. However, only the object owner can determine whether to enable or disable auditing on owner's objects as well as see some audit options for currently enabled object.

4) *Access Control*

Access controls is one of the major components of the database security. There are several access control policies in audit. The three major classes of the policies can be grouped as Discretionary access control (DAC), Mandatory access control (MAC) and Role-Based access Control (RBAC). DAC are those policies which are based on the identity of the person who requested it and on access rules which allows (or disallow) requestors. MAC policies are slightly different from the DAC in which the central authority is the head and it make sure to mandate regulations in access control. Finally, RBAC policies of access control totally depend on the roles of users in the system and what rules are giving accesses to users [14].

In this research we have found two (2) more important sub parts of access control for the betterment of IT audit quality which are Database Physical Security and Database Logical Access.

Access controls are those procedures, statements and policies that are made to allow data processing on assets only with the managements authorization. Physical and logical access controls is used to protect the important assets from unauthorized users and prevent from damage, loss or modification. The data processing needed to be protected are system software, history files, transaction detail and application programs with tables. Access to these files should be given only to authorized users to maintain a particular system.

5) *Alerts, Reports and IT Audit Quality*

The audit reporting which is installed by default is shown as follows:

i. Activity Reports
ii. Entitlement
iii. Stored Procedure Audit
iv. Alerts

This is the list of audit report installed [19]. The audit quality and the activities that are shared in these reports are of many importance. Thus, these reports are actual part of the IT Audit which will change the quality of the Audit as it should be. The report consists of many important types like Activity Overview, Data Access, and Data Modification. These reports have genuine reason to react with the quality of audit taken place in the database. So, to digest all the events that are being captured by these activities for a specific period of time will ensure that the quality of audit is low, neutral or high.

IV. Result Analysis

The following result are obtained after applying and implementing our methodology in section three that is, our proposed work.

A. Comparison against Other Models Validation Results

The objective of this validation, *Comparison against other models*, is to identify *any missing concepts* in the initial version of the metamodel and to also ensure its broad coverage. In this technique, concepts of the framework are validated and compared against concepts of other (valid) existing similar domain models or frameworks. The goal of the information security database audit and assessment framework is to express how the various models or frameworks have been tested. Specifically, database security framework will be used to generate all concepts in the initial framework.

After the Comparison of the previous models with the ISDAA Framework and from the expert reviews from the CICT UTM Database Administrator, we have the following conclusion.

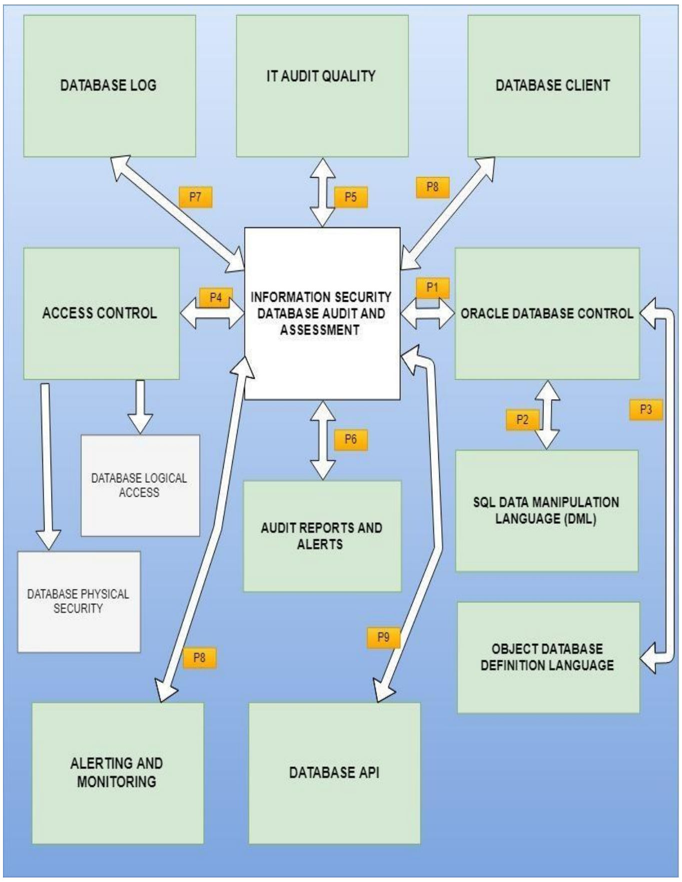


Fig. 3. Enhanced Information Security Database Audit and Assessment Framework

V. Conclusion

In this paper, the primary goal of this research was achieved by proposing a framework of information security database audit and assessment. The proposed framework will manage the quality of audit for databases in university organization. The proposed framework has been successfully validated by the respondent's university CICT staff members and upper management of the database systems. This framework can be very helpful to all database systems and their users.

Acknowledgment

The authors wish to thank the Centre for Information and Communication Technology (CICT) at Universiti Teknologi Malaysia and other related ICT experts involved for evaluation contribution of this research.

References

[1] A. Da Veiga, J. E. (2010). A Framework and Assessment Instrument for Information Security Culture. *Journal Computers and Security*, 29(2), 196-207.

[2] Archives. (2017). Identifying Information Assets and Business Requirements. In N. Archives.

[3] Brad Tuttl, S. D. (2007). An Empirical Examination of COBIT as an Internal Control Framework for Information Technology. *International Journal of Accounting Information Systems*. 240-263.

[4] Davis, C. S., & Wheeler, K. (2010). IT Auditing. In C. S. Davis, & K. Wheeler. IT Auditing, 394-397.

[5] Fielden, K. (2010). Information Security Framework, *2010 International Conference on Information Society,* 25-30.

[6] Gail Ridley, J. Y. (2004). COBIT and its Utilization: A Framework from the literature, *The Hawaii International Conference on System Sciences.*

[7] Gusti Ayu, S. I. (2014). Governance Audit of Application Procurement Using COBIT Framework. *Journal of Theoretical and Applied Information Technology*, 59(2), 342-351

[8] Jia Shi, J. Y. (2016). Research on Database Audit Scheme Design of Life Insurance Industry Based OLAP Technology, IEEE.

[9] Kehe Wu, L. H. (2014). The Design and Implementation of Database Audit System Framework, *2014 IEEE 5th International Conference on Software Engineering and Service Science*, 553-556.

[10] Lianzhong Liu, Q. H. (2009). A Framework for Database Auditing, *International Conference on Computer Science and Convergence Information Technology,* 982-986.

[11] Rouse, M. (2013, August 1). Data and Data Management. Retrieved November 20, 2017, from: http://whatis.techtarget.com/definition/information-assets.

[12] Russell, J. (2013). *What Is Auditing.* USA: ASQ Quality Press.

[13] Yang, L. (2009). Teaching Database Security and Auditing. Department of Computer Science and Engineering, University of Tennessee, 241-245.

[14] Havelka, D., & Merhout, J. W. (2013). Internal Information Technology Audit Process Quality: Theory Development Using Structured Group Processes, *International Journal of Accounting Information Systems*, 14(3), 165-192. doi:10.1016/j.accinf.2012.12.001.

[15] Stoel, D., Havelka, D., & Merhout, J. W. (2012). An Analysis of Attributes that Impact Information Technology Audit Quality: A Study of IT and Financial Audit Practitioners. *International Journal of Accounting Information Systems,* 13(1), 60-79. doi:10.1016/j.accinf.2011.11.001.

[16] L. Liu and Q. Huang. (2009). A Framework for Database Auditing, *ICCIT 2009 - 4th Int. Conf. Comput. Sci. Converg. Inf. Technol.*, 982-986.

[17] O. Cinar, R. H. Guncer, and A. Yazici. (2017). Database Security in Private Database Clouds, *ICISS 2016 - 2016 Int. Conf. Inf. Sci. Secur.*

[18] Michael A. Miller, S. K. (2016). Integrity Guide to Oracle Audit Vault.

[19] O. Cinar, R. H. G. a. A. Y. (2017). Database Security in Private Database Clouds. In: *ICISS 2016 Int. Conf. Inf. Sci. Secur.*