Center for Open Access in Science ▪ https://www.centerprode.com/ojit.html
Open Journal for Information Technology, 2020, *3*(2), 53-62.
ISSN (Online) 2620-0627 ▪ https://doi.org/10.32591/coas.ojit.0302.020530

Information Systems Audit Framework to Improve the Quality of Audit in Higher Education in East Africa

Jeremiah Osida Onunga

Turkana University College, Lodwar, KENYA
School of Science & Technology, Department of Renewable Energy & Technology

Received: 20 October 2020 ▪ Accepted: 6 December 2020 ▪ Published Online: 10 December 2020

Abstract

There are some similarities between Financial Statement Audit (FSA) and Information System Audit (ISA). FSA is an examination of the reliability and integrity of financial statement records whereas ISA is a review and evaluation of the controls, risks, and system development within an Information system infrastructure to determine if the information systems are safeguards to protect against abuse, safeguards assets, maintains data integrity, and operates effectively to achieve the organization's going concern objective. Decision makers need to ensure that the process of collecting and evaluating evidence of an organization's information systems, practices, and operations are reliable. Data manipulation can be caused by external or internal threat. Internal manipulation threat is the most dangerous one because it is committed by authorized personnel which make it very difficult to be detected. In particular, the framework introduces an anomaly detection technique, one of the data mining methods, to determine the suspected transactions arise from both internal and external threat. Once the suspected transactions are identified, procedures and monitoring control will be in place to minimize each threat. The proposed framework is expected to help both universities and ministry of higher education managers at all levels to make a vital decision based on reliable and accurate information in East Africa.

Keywords: ISA Framework, data mining framework, anomaly detection technique, higher education.

1. Introduction

Most of the organizations and firms worldwide have replaced their manual system with a computerized one in the form of information systems. These changes require a close monitoring and auditing of the data generated by such systems.

Currently higher education institutions such as universities and colleges are facing numerous challenges, for example their information systems transactions have grown in volume and complexity. These institutions exist in a highly regulated environments. Therefore, there is a convincing need for controlling and monitoring mechanisms to evaluate and validate these transactions.

The data stored in information systems in higher education institutions is of a paramount importance for both institutions as well as body represented by the ministry of higher

Correspondence: Jeremiah Osida Onunga, Tutorial Fellow and Chairman, Department of Renewable Energy & Technology, School of Science & Technology, Turkana University College, Lodwar, KENYA. E-mail: jerryosida@gmail.com.

education. For higher education institutions, they have to make sure of the integrity of the data which means the data were not tampered with whether from external sources or internal sources.

Unlike auditing in financial accounting which is concerned with the systematic verification of a company or government unit books of account transaction that is conducted by external auditors. The ISA has to ensure that the data generated and stored by information system is safeguards to protect against abuse, safeguards assets maintains data integrity and allows the firms to continue successfully. Information systems auditing (ISA) is more complex than financial auditing, because the threats can come from either internal or external sources.

Authorities in the ministry of higher education have greater role regarding the monitoring and overseeing the activities of universities. They have to ensure that the generated data by IS which are related to student marks, records, and others are accurate and not tampered with. Based on these requirements there is strong need for ISA to guarantee the accuracy of the data provided by universities to the ministry of higher education.

There are many researches provided definition for what constitute information systems auditing. For example, Lope et al. (2015) defined ISA as the assessment of various controls, risk, and system development within IS infrastructures**.**

The auditing process has moved from a manual one to a computer-based one. Recently the notion of continuous auditing (CA) has been introduced as part of ISA. CA can be defined as a comprehensive electronic audit process that enables auditors to provide some degree of assurance on continuous information simultaneously with, or shortly after, the disclosure of the information (Zabihollah et al. 2002).

Researchers have long pointed out to the importance of continuous monitoring and auditing of information system. To emphasize the importance of continuous auditing of organizational transactions a solution proposal under a new vision for organizational auditing and monitoring has been presented (Rui et al., 2012). Research on the applications of Artificial Intelligence in auditing began to increase. Kamil (2012) provides review on the main research efforts and current debates on auditors' use of artificial intelligent systems, with a view to predicting future directions of research and software development in the area.

The authors' belief that data mining, specifically outlier analysis, could be a viable approach to facilitate auditing in information system by highlighting the suspected transactions.

The main purpose of this paper is to introduce a framework for auditing information systems in the higher education. The framework aim to provide the ministry of higher education with a system that allows it to evaluate, monitor and validate university registration system transactions in a non-intrusive way. The proposed model is expected to help both university management and the ministry of higher education to systematically verify the validity of the stored information related to students. Intrusive

2. Review of literature

Non-traditional auditing tools has long being used in the audit of information systems. For instance, the use of expert system to facilitate the auditing process in information system is documented in the work of Wattiau and Akoka (1996) in which an audit expert system was developed to logistic information systems auditing.

It is understandable that most auditor professionals are lacking IT expertise which allow them to implement generalized audit software. To bridge the gap between information systems and auditors professional Shing-Han (2007) proposed a systematic analysis approach

that provides a framework for auditors to effectively understand business process and data flow/data structures of information systems.

With the vast proliferation of data stored in an electronic form, there is compelling need to ensure the validity and reliability of such data. ISA is a necessity for most organizations seeking to compete in the market. In recent years there is extensive research in ISA area with the aim of finding suitable means to ensure the reliability of the stored data. For example, Kim et al. (2015) propose a model aimed to bridge the gap between contemporary auditing practices and information system audits. The proposed model of information system audit satisfaction that includes auditor expertise and auditor role clarity as antecedent variables that affect audit responsiveness and audit reliability which in turn affect audit satisfaction.

For higher education institutions, the issues of continuous auditing (CA) and continuous monitoring (CM) of data is an important characteristic which is likely improve the reliability of the stored data and hence the credibility of the institution. Moreover, such auditing complies with the external regulations set up by the ministry of higher education. A similar work related to the continuous assurance services in information system that aim to improve the reliability of the business is presented by Marques et al. (2015). They have developed a prototype and consequent results analysis using real data which allowed them to ensure the feasibility and effective use of the proposal.

Research in CA and CM in information system remains a hot research topic. For instance, Hardy and Laslett (2015) described a case study about how CA and CM has been interpreted and implemented in a wholesale distribution and marketing company in Australia. They have obtained interesting results in which over 100 automated tests performed daily, a fully integrated exception management system, advancement from data to predictive analytics, and the use of visualization technologies for enhancing reporting.

A similar to data audit in information system is the process auditing which is a mechanism frequently used by many organizations to ensure the quality of their process. To improve the quality of audit recommendations, Kurniati et al. (2015) suggest the use of process mining in auditing business processes based on data from event logs stored in information system. Continuous monitoring (CM) of information system data from external and internal threats is of a paramount importance for top management. Many methods have been proposed to detect external intruders from accessing and hence tampering with the data. An excellent work that intends to detect external intruders is presented by (Peiying et al., 2018). They have proposed an alarm intrusion detection algorithm feature selection, weight, and parameter optimization of support vector machine (FWP-SVM-GA) based on the genetic algorithm (GA) and support vector machine (SVM) algorithm for use in a human centered smart IDS.

Internal threats can cause a huge damage for organization due to the fact that insiders have a legitimate data access. Liu et al. (2018) identified number of possible reasons which can cause enormous loss such as (1) the existing solutions do not pay enough attention on the early indications of an arising malicious insider, most of which do not raise alerts until damaging behaviors have occurred; (2) most of the solutions rely only on an individual audit data source, diminishing insights into the threats; and (3) conventional data analytics counts too much on domain knowledge in extracting features or establishing rules, resulting in a limited capability against evolving threats.

Some universities might opt for storing their data using cloud storage system. Using such approach require more rigorous auditing in order to ensure the integrity of the data. Different schemes have been proposed to address such problem, for example, Wang et al. (2018) proposed an identity-based data outsourcing (IBDO) scheme equipped with desirable features advantageous over existing proposals in securing outsourced data.

3. Information systems in institutions of higher education

In United Arab Emirates, currently there are 68 accredited universities and colleges, the majority are private institutions (www.mohesr.gov.ae). All these institutions use information systems to handle varieties of things among them the academic information related to the students. For the management of these institutions, the reliability of the generated data by these systems represent a critical issue. They have to deal with both internal and external threats. The management needs to apply close monitoring and thorough auditing of their information system to ensure the trustworthiness of their academic data. The higher education institutions specially the private one exist in a very tough competitive regulated environment which necessitate maintaining their reputation in the academic field. The ministry of higher education requires from all accredited universities and colleges to adhere to the rules and regulations set by the ministry. For the ministry of higher education there is a desperate need for mechanisms to monitor, audit, and ensure the integrity of the academic data generated by these systems.

Information system in higher education institutions has peculiar characteristics compared with other type of information systems. For example, the pattern of transactions, there are heavy transactions in certain period of time such as during student registration, student admission, and mark entries. To close the research gap, the proposed model could easily detect and highlight fraudulent suspected transactions and facilitate the decision process.

4. Methodology

Information audit relates only to the components of the information system. Because of this, information audit cannot be included within other types of audit. Information audit seeks specific objectives, has specific procedures and uses specific tools (Rus, 2012). Objectives, processes, procedures, components and international regulations regarding this process are defined by the US non-profit association ISACA (Information System Audit and Control Association). The American Standard which establishes IT governance rules is called COBIT (Control Objectives for Information and Related Technology)

Information system is composed of hardware, software, user, and data. Auditing in information system is totally different from other type of audit. In this, the auditing process will be confined to the auditing of the data or information. Ioan Rus (2015), identified and presented tools and techniques for auditing databases. For the purpose of this framework, information has seven important characteristics, these are:

Availability – the information must be available at any time during the decision process;

Integrity – the content and accuracy of the data must be in accordance with the rules and expectations of the organization;

Compliance – the logical structure of information and its concrete values must reflect the actual level of processes it characterizes;

Reliability – the information must relate to the specific decision-making process that is served;

Efficiency – the information must be provided with the lowest consumption of resources;

Effectiveness – the information must be relevant, accurate and timely provided for decision making;

Confidentiality – the information must be provided only to users whom they are intended to be delivered.

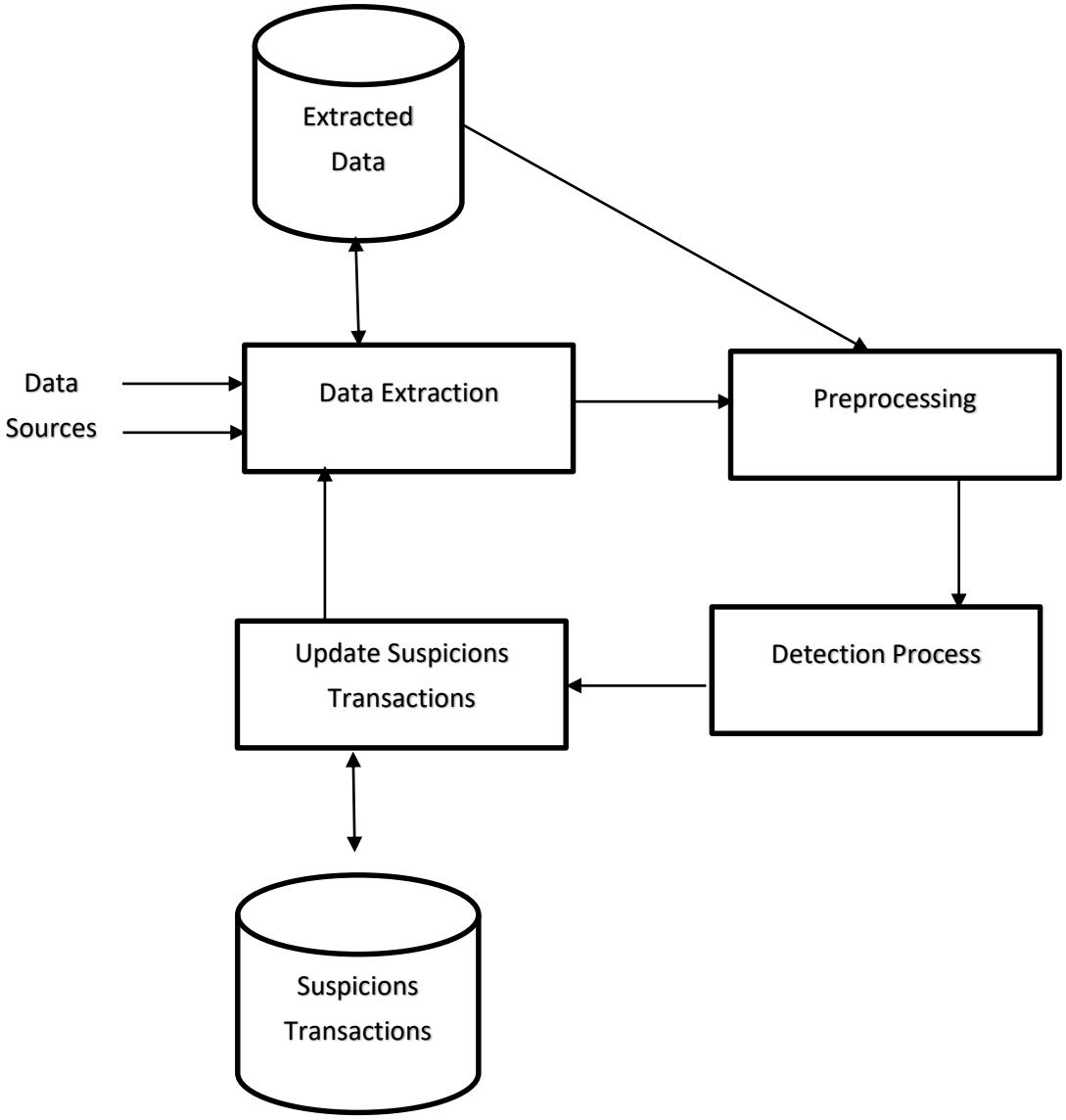

Figure 1: The proposed Framework Processes

Figure 1 above shows the proposed framework processes that uses data mining techniques to audit and detect the suspected fraudulent transactions that can be referred to the management of the higher education institution and the ministry of higher education.

The proposed framework indicates that there are five phases which are:

Data Extraction Phase

This phase uses information system log file to perform data extraction and preparation and the extraction of valuable features in detecting suspected fraudulent transactions.

Data Pre-processing Phase

The step accomplishes data pre-processing which may include data cleaning, normalization, transformation and feature selection to prepare the data for analysis.

5. Detection Process Phase

The phase, as shown in Figure 1, includes two processes:

- Mining: This phases uses a suitable outlier analysis algorithm to detect the fraudulent suspected transactions.
- Post processing: This phases intends to evaluate the generated patterns after the mining process.

6. Generating fraudulent suspected Transactions Phase

This phase uses the tested pattern to generate the fraudulent suspected transactions. This phase is the actual experimental work. The result will be delivered to the institution management for further investigations.

These steps or phases will further be detailed when the actual data is prepared and the model will be tested.

Conceptual Design of the Proposed Framework:

Figure 2 shows the conceptual design of the proposed framework. The proposed design consists of the following services/components:

User Interface Service/Component: helps the users to navigate the different services including the Naming and location service/components, Detection service/Component

Reporting Service/Component, Data Sources and Suspicious Transactions Database.

Naming and Location Service/Component: this service stores information about the names and locations of the registered services. This service can be implemented as a centralized or distributed service.

Detection Service/Component: This service can be implemented as an extensible class that can be extend by the developer to add a new detection service such as detection service for the academic institution and another one for the regulatory institution.

Reporting Service/Component: this service is used to store suspicious transaction in a special database that can be accessed and investigated by different users through the user interface service.

Data Sources: these are the Databases and files that includes information about the academic regulations, registration information, policies, processes/procedures, student information and regulatory rules and any other data that is relevant to the purpose of audit.

Suspicious Transactions Database: this database stores only the suspicious transaction detected by the detection service. This database can be implemented as a centralized or distributed database as required.

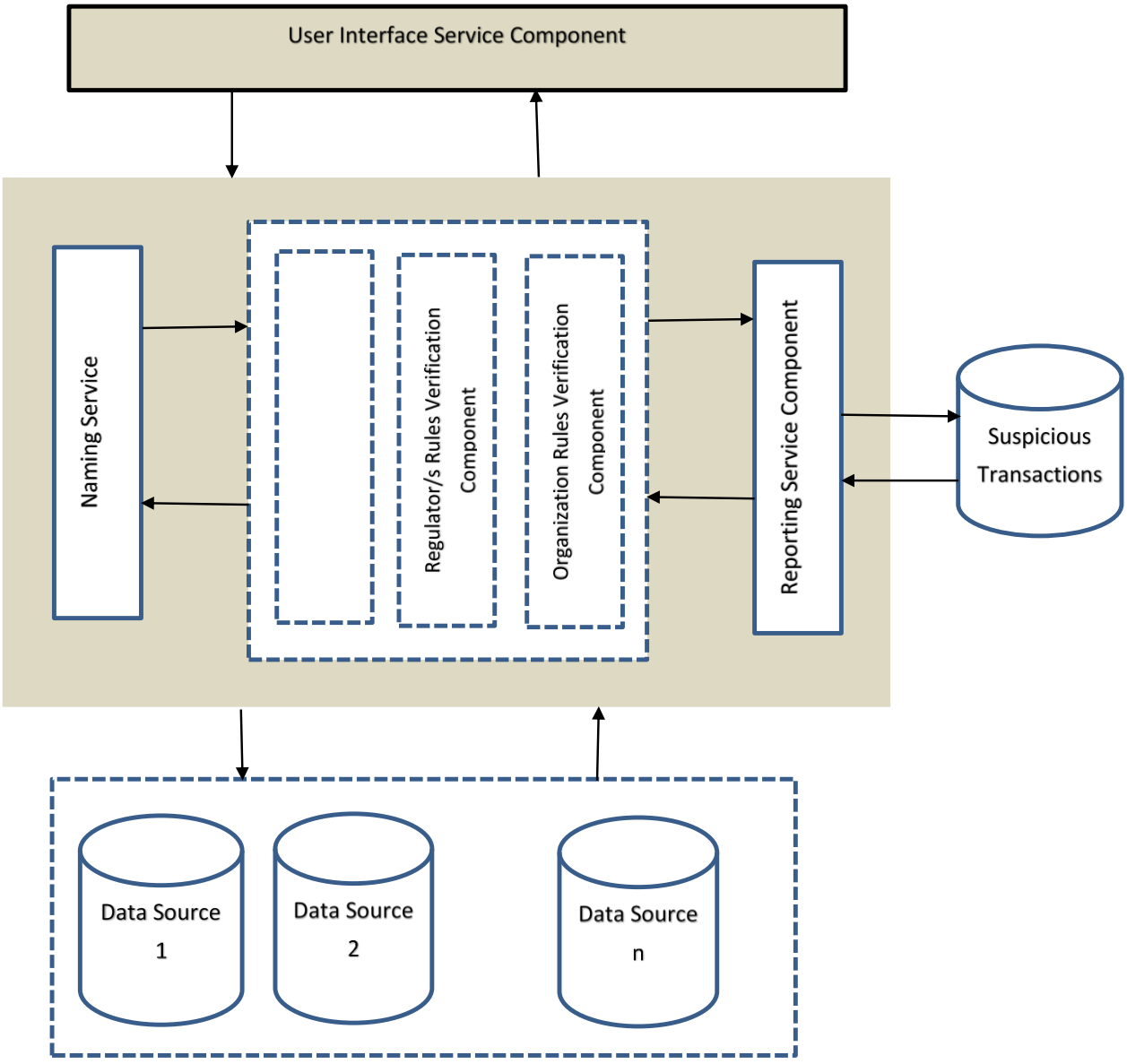

Figure 2: The Proposed Framework Components Design

7. Discussions

Internationally, universities recognize the importance of university registration systems, one of the categories of information systems. These systems store huge amount of data

related to students, courses, grades, etc. Maintaining the integrity of such data is of a paramount important for both universities and ministry of higher education. One of the responsibilities of the ministry of higher education is to oversee and monitor the activities of universities and has to guarantee the accuracy of the data stored by such systems.

Information system audit represents a challenging issue for most organizations specially higher education institutions in which the good reputation of such institution plays an important role in improving the market share for these organizations. Maintaining data integrity is an important characteristic sought by most organizations operating in a very competitive environment. The audit framework aims to establish whether university registration systems are safeguarding corporate assets, maintaining the integrity of stored and communicated data, supporting university objectives effectively, and operating efficiently. To achieve such uphill task, the framework algorithm first extracts the transactions from the university registration system and then utilizes outlier analysis (Han et al., 2012), one of the data mining techniques, in order to identify the possible fraudulent transactions. The algorithm takes into consideration the different types of events, stages, and relationship that constitute the essence of each university registration system transaction.

It is recognized that university registration systems have peak period time during which there are heavy transactions that can be generated. For example, during registration at the beginning of the semester and at the end of the semester where students marks and grades will be recorded by the instructors and employees of the registration office. The framework uses different factors to identify the suspected fraudulent transactions. One of the most important factor is the timing of the transactions. In university registration system, some transactions can only be generated during certain period of time. For example, transactions related to student marks and grades, such type of transactions should only occur at the end of the semester or within certain period of time and should be performed by certain types of users. If the auditing system detects that such transactions were generated outside these times, immediately the system flags these transactions as suspected fake transactions, and hence should be inserted into the file of the suspected fraudulent transactions for further investigation.

Factors other than the timing that should be taken into consideration by the framework in the auditing process is the transactions that violate university or ministry of higher education rules and regulations. Such types of transactions should be marked as suspected deceitful transactions and hence should be inserted in the file of the fraudulent transactions.

Another important factor that can contribute in the identification of improper transaction is related to the location from which the transactions were executed. Most universities allow the execution of transactions related to student marks and grades from certain locations. Any transactions carried out by individuals outside these locations should be flagged by the auditing system as being suspected fake transactions and hence should be inserted into the file of the suspected fraudulent transactions for further investigation.

The framework also aims to address issues related to transactions which appear as if they are legal, but in reality, they are fake one. For example, transactions performed by authorized personnel from the right place, from the right machine, and at the right time, but nevertheless they might be fraudulent. This is an example of internal threat. Then how the framework addresses such type of threat. The framework can respond to a threat of this kind by using the concept of transaction consistency. In such scenario, transactions can be grouped based on certain characteristics. For example, an instructor completed entering the marks of the students for certain course section, if the auditing system discovers that some transactions were updated by another user other than the instructor, these transactions will be highlighted by the system as being suspected fake transactions and will be recorded into the file of the suspected fraudulent transactions for further investigation.

8. Conclusions and future research

Prior research in continuous auditing (CA) and continuous monitoring (CM) of data demonstrates the existence of solid connection between contemporary auditing practices and information system audit. With the objective of ensuring the validity and reliability of all data stored in an electronic form, the information system audit will remain a controversial research topic. This paper highlights the theoretical aspects of a framework that will be used to detect and identify fraudulent suspected transactions in an information system for higher educations. Based on the literature that we have reviewed, we found that this is the first attempt to propose the use of viable technique, outlier analysis algorithm, to improve the auditing of information system.

In this paper, we have just proposed a theoretical framework to support information system audit in higher education. The findings of our research contribute to the previous literature in various ways. First, the consequences of this research contribute over-all support to the recommendation that all else remain constant, the higher the quality of the data, the better the performance of all organization. Identifying fraudulent suspected transactions in an information system for higher education help both university and ministry of higher education senior excusive to make a complex diction in using resources more efficiently and effectively and ensure education quality.

We have to acknowledge at this point that there is a need for further investigation to discuss how to implement this framework using real data that should be collected from university's information system. Moreover, the outlier analysis, the proposed data mining technique, employs different type of techniques to detect the outlier objects. Among the techniques that employed by outlier analysis clustering-based techniques, nearest-neighbor classification techniques, and statistical methods. There is a convincing need for future research to decide which is the best outlier analysis technique that can be chosen for improving the auditing of information systems.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public commercial, or not-for-profit sectors.

The author declares no competing interests.

References

Comyn-Wattiau I., & Akoka, J. (1996). Logistics information system auditing using expert system technology. *Journal of Expert Systems with Applications*, *11*(4), 463-473.

Han J., Kamber, M., & Pei, J. (2012). *Data mining concepts and techniques*. Morgan Kaufmann: Waltham, MA 02451, USA.

Hardy, C. A., & Laslett, G. (2015). Continuous auditing and monitoring in practice: Lessons from Metcash's business assurance group. *Journal of Information Systems*, *29*(2), 183-191.

Kim, S. L., Teo, T. S. H., Bhattacherjee, A., & Nam, K. (2015). IS auditor characteristics, audit process variables, and IS audit satisfaction: An empirical study in South Korea. *Information Systems Frontiers*, November 2015, 1-15.

Kurniati, A. P., Kusuma, G. P., & Ary Wisudiawan, G. A. (2015). Designing application to support process audit using process mining. *Journal of Theoretical and Applied Information Technology*. *80*(3), 473-480.

Liu, L., De Vel, O., Han, Q-L., Zhang, J., & Xian, Y. (2018). Detecting and preventing cyber insider threats: A survey. *IEEE Communications Surveys & Tutorials*, 20(2), SECOND QUARTER 2018.

Lope, A. R., Islam, & Ai-Nemrat (2015). *Measuring sustainability for an effective Information System audit from public organization perspective*. 9th IEEE International Conference on Research Challenges in Information Science, IEEE RCIS 2015; Athens; Greece; 13-15 May 2015; Category number CFP1540D-ART.

Marques, R. P., Santos, H., & Santos, C. (2015). Monitoring organizational transactions in enterprise information systems with continuous assurance requirements. *International Journal of Enterprise Information Systems*, *11*(1), 13-32.

Marquesa, R. P., Santosa, H., & Santos, C. (2012). A solution for real time monitoring and auditing of organizational transactions. *Procedia Technology*, 5, 190-198.

Omoteso, K. (2012). The application of artificial intelligence in auditing: Looking back to the future. *Journal of Expert Systems with Applications*, *39*(9), 8490-8495.

Rezaee, Z., Sharbatoghlieb, A., Elam, R., & McMickle, P. L. (2002). Continuous auditing: Building automated auditing capability. *AUDITING: A Journal of Practice & Theory*, *21*(1).

Rus, I. (2015). Technologies and methods for auditing databases. *Procedia Economics and Finance*, 26, 991-999.

Shing-Han, L., Shi-Ming, H., & Yuah-Chiao, G. L. (2007). Developing a continuous Auditing Assistance System Based on Information Process Models. *The Journal of Computer Information Systems*, 48, 1.

Tao, P., Sun, Z., & Sun, Z. (2018). An improved intrusion detection algorithm based on GA and SVM. *IEEE Access*, 2018, 13624-13631.

Wang, Y., Wu, Q., Qin, B., Shi, W., & Deng, R. H. (2017). Identity-based data outsourcing with comprehensive auditing in clouds. *IEEE Transactions on Information Forensics and Security*, *12*(4), 940-952.