sciendo
Control and Cybernetics
vol. **51** (2022) No. 3
pages: 389-419
DOI: 10.2478/candc-2022-0022

Readiness of low complexity ERP for continuous auditing in SMEs: The Brazilian case study*

by

Rosana Carmen M. Grillo Goncalves[1] **and Joshua Onome Imoniana**[2]

[1]University of São Paulo, Av. Bandeirantes 3900, Ribeirão Preto - SP, 14040-905, Brazil
[2]University of São Paulo, Av. Prof Luciano Gualberto 908, Sao Paulo - SP, 05508-010, Brazil

Abstract: The continuous auditing technology assures integrity of accounting systems and consequently improves the decision-making process of the small and medium-sized enterprises (SMEs) that implement it. Considering that SMEs located in developing countries function within a more risk prone environment and do not have resources to implement all layers of customized corporate functions in information systems, one argues for their reliance on the features of low complexity of enterprise resource planning (ERP) software to benefit from continuous auditing (CA). The purpose of this study is to relate the understanding of the CA demands and low complexity ERP systems' technical functionalities in SMEs. Thus, to fulfill this objective, a conceptual model has been drawn to integrate the key concepts related to CA. Four pillars are the core of this model, namely: segregation of duties (SoD) with role-based access control centered on process-based approach (PBA); internal checkpoints; audit trails; and the level of integration of the continuous auditing software. This model was validated through the benchmarking of the implementation of the pillars in three cases of low complexity ERP systems adopted by SMEs in a developing country. The benchmarking/results of the study show significant differences between operational mechanisms of the three ERP software. Namely, the role-based access control exists in the two of the ERP_LC but not in the Brazilian one. Also, there is no check-point in the Brazilian ERP_LC and it does not integrate with continuous audit features. This study distinguishes between the low complexity ERP's functionalities and the features of a more complex environment, thus bringing an important contribution to the study of low complexity ERP's readiness for continuous monitoring in SME's internal auditing processes.

*Submitted: August 2021; Accepted: September 2022.

Keywords: internal audit, continuous auditing, internal control, low complexity ERP, SME

1. Introduction

Every organization is exposed to risk, primarily with respect to the achievement of its business goals. The risks include operational, financial, geopolitical, technological, legal, environmental and compliance risks, to mention just the most important ones. In a nutshell, normally the independent auditors summarize them into inherent, internal control and detection risks. Whatever the nature of risk, in order to minimize the exposure, it is imperative to implement risk control mechanisms that ensure its reduction to an acceptable threshold, which provides an optimal compromise between the cost of implementation and the risk reduction achieved. Internal controls implemented by organizations have been traditionally used to mitigate risks that are incident on any operation. These risks may be due to internal control flaws arising from the misuse of operational software, errors in the performance of activities, and circumvention for perpetration of fraud, or unintentional wrong segregation of duties (SoD). Kobelsky (2014) suggests a comprehensive view of SoD and the risks associated with deficient segregations of incompatible duties.

With the contemporary technology at hand, the respective internal controls have been improved so as to act in real-time or close to real-time. Some functionalities of continuous monitoring, otherwise referred to as continuous auditing, enable internal auditors or managers to mitigate operational risks, which sustains the process-based approach. The process-based approach is a management approach that views a business as a collection of processes, managed to achieve a desired result (Blessing, 1994; Bagheri and Hjorth, 2005). In the final analysis, it provides higher quality of, in particular, financial statements to users for an end of a period of the operational process. Thus, to enhance the monitoring processes the continuous audit (CA) occurs within the shortest possible time after the occurrence of an event in a control environment. According to Davidson, Desai and Gerard (2013), relative to periodic auditing, properly designed continuous auditing tools increase the appropriateness of evidence by improving the accuracy, timeliness, relevance, and breadth of information used in judgments and decision-making.

In effect, there are different levels of technological sophistication in creating real-time internal controls that minimize operational risk. But this sophisticated reality cannot be transposed to low complexity ERP (ERP_LC) systems neither can it correspond to the reality of internal controls in SMEs. Therefore, the set of controls that will be studied in this article includes some less sophisticated functionalities of continuous process monitoring, including continuous data auditing. In Bumgarner and Vasarhelyi (2015), these are considered the most basic types of technological disruption in accounting and auditing. A more complex approach involves presenting monitoring and risk assessment

using algorithms that encapsulate refined probabilistic models and even more sophisticated continuous compliance monitoring involving creation of regulatory compliance taxonomies.

The SMEs internal auditing processes are used to assure compliance with the laws and regulations and to achieve certain objectives, concerning (i) operations of the business, (ii) reliability of the financial statements, (iii) safeguarding of the assets of the business (Daniels, Ellis and Gupta, 2013). The controls in SMEs cannot be truly sophisticated inasmuch as there is no rigor of an internal audit committee as this takes place, for instance, in large publicly traded companies. According to DeZoort and Harrison (2018), the essential need of an SME is a properly functioning internal control procedure that can help limit or even eliminate the opportunity for fraud to take place, as well as to remove redundancies and to improve control in business processes.

The life cycle of many SMEs may be explained by certain characteristics that are related to the lack of internal controls. In Brazil, more than half of the small and medium-sized enterprises have a reduced life cycle, varying from one to five years (see Santos, Silva and Neves, 2011; Imoniana et al., 2011; Vaz and Espejo, 2015). These authors try to explain the failure of these enterprises using many factors, one of them is the lack of control consciousness. The diffusion of internal control procedures in Brazil can be an important factor of viability, competitiveness, and growth of such firms. Thus, this study investigates the technological resources for Brazilian SMEs to implement feasible controls. In view of closing the existing research gap, this study examines the following research question: *what are the basic features of ERP_LC that make them ready to be used by small business owners in view of exploring the continuous monitoring procedures*?

After this introduction, the rest of this article is structured as follows: Section 2 reports on underpinning literature, Section 3 deals with the design of the study, this being followed in Section 4 by the presentation of the modeling pillars of control of Low Complexity ERP systems. Then, to sum up, we present in Section 5 the benchmarking and results, in Section 6 the discussion, and finally, in Section 7, the concluding remarks.

2. Underpinning literature

2.1. General background

In Bumgarner and Vasarhelyi (2015), continuous auditing is defined as a process and as a technology. The most relevant technological aspect is the provision of continuous audit software, which is responsible for testing the flow of data contained in audit trails, and comparing it with standards or benchmarks to detect anomalous situations (Kogan et al., 2010). In continuous auditing process, relevant discrepancies found generate alerts, which are forwarded to those in charge of internal control. Generally, these persons are termed the systems owners, and

they are charged with the systems responsibilities and accountabilities regarding the outcome.

According to Alles et al. (2006a), the basic levels of continuous audit benefit from the continuous monitoring of business process controls as an important subset of the continuous audit with relevance linked to the prevention of internal errors. This audit makes use of resources already present in some ERP systems, particularly data from system audit trails, which, however, need to be further processed. Continuous data auditing, as a subset of continuous auditing, can reduce the cost of internal control. By increasing the effectiveness of the audit process, they contribute to reduction of errors and fraud, which, in turn, tends to increase the value of the business. In this way, the respective process is no longer considered as having a low-value aggregation (Rikhardsson and Dull, 2016).

Evolving from the classification presented in Brown, Wong and Baldwin (2007), the studies following the mainstream research in CA (Lenz and Hahn, 2015; Eulerich and Kalinichenko, 2018) can be classified into two categories. It must be stressed that these two categories do not embrace all of the research performed regarding CA, they only represent two clusters of similar approaches.

The first one stresses the proposition of technological solutions, or of enabling technologies, to improve CA possibilities (Li, Huang and Lin, 2007; Alles et al., 2008; Van der Aalst, et al., 2011; Kim and Kogan, 2014; Kogan et al., 2014; Gómez-López, Gasca and Pérez-Álvarez, 2015; Ly et al., 2015; Gershberg, 2016). These studies represent a research paradigm that calls for the creation of new artifacts to solve practical problems, absorbing different processes and research methods from design science (Hevner and Chatterjee, 2010).

The second research approach also considers technological resources and additionally embraces the organizational context and the local culture as well as professional profiles that influence continuous auditing adoption (Gonzalez, Sharma and Galletta, 2012; Vasarhelyi et al., 2012; Bierstaker, Janvrin and Lowe, 2014; Li et al., 2018; Mokhitli and Kyobe, 2019). These studies emphasize internal auditor's attitude towards the use of information technology for continuous auditing and other organizational and cultural concerns. For example, in their interview study with internal auditors, Vasarhelyi et al. (2012) examine the status of CA adoption and find that the support by the management and the employee's expertise of the technology are influential factors of this adoption.

Related to the first category that emphasizes enabling technologies, there are some papers that directly address the embedding of CA or CA-related techniques in ERP systems. Debreceny et al. (2005) investigate the implementation of embedded audit modules (EAM), which provide the technical basis for continuous monitoring and CA in the existing ERP systems. Alles et al. (2006a) give an overview of the practical implementation of a CA approach at Siemens, described as SAP R/3 centric. They report the development of an approach to

implement the monitoring and control layer for continuous monitoring of business process controls and the lessons learned in these processes, giving emphasis to the administration of audit alarms.

Kuhn and Sutton (2010) extend the discussion of Debreceny et al. (2005), bringing into analysis the ERP technological resources to implement CA with EAM and also with middlewares solutions that work independently of the ERP system. Shin, Lee and Park (2013) present case studies of actual continuous auditing systems based on continuous monitoring, implemented in the financial industry and in the manufacturing industry. Their emphasis is on the method of implementing the continuous auditing system in the enterprise resource planning (ERP) environment. More recently, Singh et al. (2014) discussed continuous auditing and continuous monitoring, bringing empirical evidence from actual implementations considering three different ERP systems from different software houses. Haynes and Li (2016) recognized that ERP systems have become the standard technological platform for business operations and present anti-fraud audits using continuous auditing process that use the ERP functionalities in a case study of an energy industry company in Texas. They indicate that lower fraud risk and higher efficiency are the benefits obtained by using CA implemented in an ERP system.

As observed by Antunes et al. (2010), in Brazil there is the predominance of the use of ERP systems for the control through cost centres (63%) and for the profitability analysis of the activities by sectors (41%), while, for instance, in Greece, ERP mostly envisage internal audit (69%) and the obtainment of non-financial performance indicators.

Rikhardsson and Dull (2016) provide evidence that continuous auditing in Europe has been effectively used by small firms. Their findings include cases in which, as soon as supervisors had audit trails and tools for their use, they initiate the use of such tools, seeking rather the mitigation of errors than the detection of fraud. Although this paper studies CA in small businesses, its focus is on the organizational impact of these artifacts and not on their technological feasibility.

Our paper intends to fill this specific literature gap by discussing functionalities adequate or proper to the implementation of continuous audit modules in low complexity ERP systems adopted by small enterprises.

2.2. Internal control and low complexity ERP in SMEs

Small and medium-sized enterprises (SMEs) or small businesses can be defined as independently owned businesses or companies with a limited number of employees (Baker, Grinstein and Harmancioglu, 2016). Many studies bring the number of employees inferior to 500 as defining small business (Lu and Beamish, 2006; Munro, 2013; Batra et al., 2015). SMEs play an important role in the

socio-economic development of nations by creating jobs and boosting economic recovery (Coyte, Riccieri and Guthrie, 2012).

Manolova, Manev and Gyoshev (2010) found that process standardization is positively associated with the degree of internationalization and growth of SME firms. In Brazil, it is common for an SME to act as producer of critical components having to fit their clients' needs, sometimes expressed as rigorous specifications. Cahen, Lahiri and Borini (2016) studied Brazilian SME new technology-based firms and identified as barriers the internal organizational capacity and human resources. Also, there is a suggestion to improve suppliers' collaboration or to make an organizational effort aimed at the standardization and/or redesign of business processes, and the SMEs have adopted ERP_LC systems that happen to be one of the primary vehicles to help to solve such problems (Zadeh et al., 2018).

The low complexity ERP systems consist of software components, also called modules, that focus only on five essential business functions: (i) production planning, (ii) finance and internal control, (iii) HR, (iv) sales and marketing, and (v) purchase. At the same time, these are the systems, which the independent auditors get mostly concerned about when analysing the business cycle for the true and fair view of the financial statement. The respective systems are less complex than other ERP systems, which are developed to offer functionalities for improving quality control, customer relationship management (CRM), supply chain management, reversal logistics and for improving other sophisticated business processes. Jituri, Fleck and Ahmad (2018) emphasize that an ERP_LC system is proper for small and medium-sized enterprises that require: # shared data and visibility across the main areas of the company; # the possibility to manage all departments from production to distribution and accounting in one integrated system, and # information about inventory availability, suppliers, and customers.

Deep et al. (2008), Poba-Nzaou and Raymond (2011) and Haddara and Zach (2012) describe different aspects of the ERP_LC selection and adoption process. An important phase is the definition of functional requirements described as a part or as an important input of the selection process (Illa, Franch and Pastor, 2000; Deep et al., 2008; Asgar and King, 2016). The essential business areas have stakeholders that will be given an ERP_LC, which they are supposed to adopt and use. In general, examining and coordinating the needs of these areas and of the general administration will result in a checklist of requirements. Each ERP_LC system will have their capabilities evaluated against the identified requirements, being calculated within the final evaluation score.

An enterprise with an ERP_LC will have most of the accounting postings fulfilled in a preconfigured way, without manual journal entries, increasing, therefore, the effectiveness of the internal controls and finally the quality of the financial statements. The minimization of manual journal entries will make the firms less vulnerable to errors. In addition to vulnerability, accounting manual

journal entries tend to have higher values when compared to automatic journal entries, which also implies severity with respect to controls. Muhrtala and Ogundeji (2013, p.13) conclude that the most significant security threats to accounting are: (i) the accidental manual entry of wrong data, (ii) the accidental destruction of data by employees, (iii) their habit of sharing access credentials, implying an unauthorized access to the software and unauthorized data extraction. The same assessment is corroborated by Wang et al. (2019), and in the same vein, Findilkli et al. (2019) state that managers' perception of information technology sophistication value to SMEs includes financial fraud detection among other perceptions related to insights associated with the increase of the value of business operation.

Unfortunately, not all ERP_LC have the proper functionalities and features to implement continuous process monitoring including continuous data auditing. Knowing that the selection and implementation of an ERP_LC system presents a huge challenge for SMEs (Deep et al., 2008; Zadeh et al., 2018), our paper goes further to discuss the basic functionalities that an ERP_LC needs to afford internal controls capabilities, particularly to SME that processes a high volume of transactions.

The concept of Segregation of Duties (SoD) has always been present in the discussion of internal control, particularly now that the implementation of Foreign Corrupt Practices Act (FCPA) and the Sarbanes Oxley Act (SOX) for the traded companies becomes a *sine qua non* condition. According to COSO (2013), segregation of duties should: "divide or allocate tasks to multiple individuals so that the risks of fraud and error are reduced". Minimizing the involvement of one single person in a transaction cycle that leads to transference of wealth is the objective of segregation of duties of those who originate, from those who countercheck and those who authorize, say, payments. SoD prevents an individual from having access to the system so widely as to enable him or her to perform all the transactions that make up a business process that updates the general ledger, without being subject to satisfactory checks and balances. Internal controls should promote SoD to safeguard assets, mitigating fraud, involving the diversion of services, products, and assets (Singh et al., 2011; Imoniana, Feitas and Perera, 2016). Concisely, in processing a transaction, the basic SoD control divides key functions. These functions may include: a) creation and / or origination of transaction records, b) internal checking, (modification and deletion), c) authorization, d) update of posting accounting records, and e) monitoring.

Role-based access control is crucial in an ERP_LC for allowing effective segregation of duties. Role-based access is construed on the authorization procedure. It is commonly embedded in many systems and thus provides the simplest way to control the access to parts of the data storage (Wolter, Miseldine and Meinel, 2009). All employees assigned to the same role will be allocated the same access profiles. The administration of profiles, as clusters of users, requires formal rules

and facilitates the control. Although many employees can be linked to the same role, each access will be individually controlled.

As put forth by Imoniana et al. (2011), access permissions should be given on a need-to-know basis. There should be minimal data governance, with the responsibility of profiling users. An employee should be aware that he is not authorized to pass his access permissions to third parties. Clear rules should be disseminated, characterizing the use of alien identification as misappropriation, even if such use has been previously authorized. In a pedagogical way, users should know that if there is identity theft, that is, if a user steals other's identification information, and engages in incorrect or fraudulent acts with this identity, they will be liable for their acts, even criminally (Singh et al., 2013).

2.3. Checkpoints

Some micro-functions are interdependent, that is, for a business process to be completed it is necessary for them to be "consolidated". In general, sequential execution of such micro-functions will be improved if an ERP_LC forges the synchronization using clearing or transient accounts so that consolidation occurs after the last micro-activity.

Such synchronization may facilitate the inclusion of checks and balances. This occurs, for example, when the execution of the activity in t_1, gives rise to numbers that must be identical to other values generated by the activity in t_0. Using clearing or transient accounts, if there are discrepancies, process failures can be detected in real-time (Alaküla and Matulevičius, 2015).

The synchronization and inclusion of checkpoints are crucial for high-quality financial reports. Clearing accounts can be understood as transient or interim accounts, created to keep open the values of activities / transactions that have not yet been consolidated, and zeroed out at the end of the transaction. An example of this occurs when companies transferred money between their bank accounts A and B, from different banks through check deposit. On day d_0 the amount exits from account A and on day d_1 the amount enters into account B. If the accounting was not done in real-time, the recording of this transaction would only occur after day d_1 and would be done directly: a debit to the account B, a credit to the account A. However, ERP systems handle the real-time recording of every activity. Therefore, in d_0 the posting must be done: a debit to the transient account, a credit to the account A. In d_1 another posting must be done: a debit to the account B, a credit to the transient account. This mechanism is responsible for the synchronization of two activities necessary for the money transfer process. On the other hand, if the bank clearing system were to fail and the value that has been taken from account A were different from the value entered into account B, such inaccuracy would be detected at d_1, once the value of the transient account would be different from zero. In this transaction, a checkpoint was included in the second accounting posting (Schultz, 2013).

2.4. Audit trails and error detection software

Audit trails, and notably audit logs, are files or tables that contain the record of the activities of software users. The main component of audit trail is the *event log* (Jans, Alles and Vasarhelyi, 2014). It can include an entry for each operation applied to a database: – which rows user created, modified, or excluded in tables with master or transaction data file; it can also include the account number of the user and online terminal to be applied to each transaction recorded in the log.

The most distinctive characteristic of an event log is how much metadata it has and how efficiently its metadata permits tracing relationships with other events. The audit trails are supposed also to record the successful and unsuccessful access attempts to the system (Wang et al., 2019). Additionally, it is intended to establish a chronological order of steps necessary to move from the beginning of a transaction, corresponding to a business process, to its completion.

Considering that there are firms, in which ERP_LC processes hundreds of thousands of transactions per day, the enormous size of audit trails cannot be properly and on time handled by human beings. Therefore, audit trails constitute the input of the anomaly detection software used to detect possible fraudulent activities. Denning (1987) introduced the use of audit trails to detect atypical user behaviors. Most models aim to track records, looking for the pattern's deviations (Gershberg, 2016). Monitoring involves the separation of normal activities from suspicious activity and may be: (i) periodic, (ii) when necessary, that is – when triggered by a critical event; or (iii) continuous. With this continuous approach, the audit occurs within the shortest possible time after the occurrence of an event, minimizing the consequences of a potential deviation. Numerous alerts and warnings can be generated by the anomaly detection software, and only a minority should be investigated more carefully for the detection of errors or fraudulent actions (Alles et al., 2006a; Alles, Kogan and Vasarhelyi, 2008; Kuhn and Sutton, 2006; Eulerich and Kalinichenko, 2018). Anomaly detection software tends to generate many false negatives in situations, in which the tests performed indicate that there are no signs of abnormality although there are, in fact, errors and frauds. False positives can also be displayed when legitimate transactions are classified as fraudulent. Nevertheless, application of machine learning may be able to minimize the false negatives arising from anomaly detection.

The detection of deviance from patterns requires the use of statistical methods and outlier tests. After identifying the data distribution type, different statistical calculations will be required for the identification and treatment of outliers (Lee, Kim and Rhee, 2001; Veasey and Dodson, 2014). To improve the alerts, it would also be important to require the intervention of the internal auditors, who not only define the initial criteria to be implemented in the algorithms, but also review them periodically. The perfecting of the algorithms

grows in relevance in proportion to the increase in the volume of alerts produced by huge data sets of transactions, that need to be interpreted in real-time. So, one can infer that with the use of big data, the perfection of the control algorithms would be continuous as the adoption of continuous auditing grows.

2.5. Levels of integration of the anomaly detection software named continuous auditing (CA)

Generally, two approaches define possible architectures for anomaly detection software to work in partnership with the company's systems. They are, namely, the approach of encapsulated audit modules (EAM) and the monitoring control layer (MCL). By implementing the EAM approach, the source code, generated from the algorithms with comparisons and emission of alarms, is developed and implemented within the integrated transaction processing corporate system, having direct access to the data and using the same database management system. The storage of alarms is done in the same database, in which the transactions are stored (Groomer and Murthy, 1989; Kogan et al., 2010).

Vasarhelyi, Alles and Kogan (2004) introduced the concept of the monitoring control layer (MCL) architecture as an alternative to the embedded model. The MCL can be defined as a middleware solution that works independently of the integrated transaction processing corporate system.

If the integrated transaction processing corporate system or the ERP system provides an audit trail, the MCL will not be responsible for extracting data, but only for their analysis (Best, Rikhardsson and Toleman, 2009). The audit software with MCL architecture is not usually being developed by the integrated transaction processing corporate system developers, but by third parties. According to Rikhardsson, Singh and Best (2019), organizations do increasingly buy the generalized continuous auditing solutions from vendors rather than developing their own tools. Leading traditional software products with anomaly detection capabilities, are usually referred to as general audit software. Such products are provided, for instance, by ACL software company (ACL analysts, ACL Essentials), and by Caseware Analytics (Idea, CaseWare Monitor). There are pieces of evidence that small and medium-sized firms will choose a less robust and cheaper solutions (Rikhardsson and Dull, 2016).

3. Research design

The concept of low complexity ERP's readiness for continuous monitoring evaluation model was preceded by an extensive bibliographical review of key ideas and notions, related to continuous auditing and of the proposed technological solutions to improve CA possibilities, particularly those related to ERP and ERP_LC systems. The concept of technology readiness is in consonance with

Clausing and Holmes (2010, p. 52), for whom technology readiness ensures that products will perform as expected in the user's environment.

To initiate the evaluation model validation, we selected the cultural and social context of small enterprises, associated with Brazil, a developing country; with a particular interest in the evolution of corporate internal controls, where anti-frauds initiatives have been recently intensified (Valarini and Pohlmann, 2019).

3.1. Choosing the low complexity ERP systems for the benchmarking

To proceed with the validation of the proposed model, three different software houses of ERP_LC systems products were chosen to be evaluated.

In Brazil, exaggerated tax complexity poses risks related to fiscal and accounting configuration, responsible for making the particularities of the organization to be compatible with the global ERP_LC systems‘ options. So, a Brazilian local ERP_LC system was chosen, in particular, owing to a standard for the tax compliance. Besides, all of the chosen products were expected to have the basic functionalities of an ERP_LC system in different modules or condensed in macro modules: Purchasing, Warehouse Control or Inventory Management, Sales, Production Planning and Control along with Cost Control, Finance (including Accounting, Treasury and Fixed Asset Management) and Payroll.

It is noteworthy that the global ERP_LC systems are commonly commercialized in Brazil with the inclusion of local Payroll, Tax calculations and reporting modules, that provide full compliance with Brazilian legislation. Let us also remark that the two global ERP_LC systems chosen demanded more configuration and parametrization effort. Their implementations were more complex and required more attention considering that manual error is stochastic, while errors in the parameterization of the software are deterministic and will always occur if one does not mastermind the respective concepts.

In all three products chosen, the Production Planning and Control module was quite limited, fitting *make-to-stock* mode of production, in component assembly manufacturing processes, as usual in these class of products (Powell, Riezebos and Strandhagen, 2013, Gupta et al., 2014).

The first product selected was Sap Business One (SAP B1), from SAP, the world's leading ERP systems company, offered as a small and medium-sized enterprise SAP product. The other two were Odoo, an open-source ERP, and a Brazilian product, which will be called Brazilian local ERP_LC, which is among the top five sold in the country for small and medium-sized firms. SAP B1 and the Brazilian local ERP_LC have comparable costs and market shares.

Odoo, otherwise formerly known as OpenERP, is a system that has been used worldwide, with versions available for Microsoft Windows, Linux, and Mac OS. Version 7.0 for Microsoft Windows, with PostgreSQL as the database man-

agement system, was used in our study. Open-source software, as well as free software provides free source code to interested parties, however, it goes beyond that, demanding efforts in the organization and integration of the development process, aiming at offering a single package with specific versions (OSI, 2016). Such coordination is essential, considering that there is an entire community involved in the development of Odoo and that there are numerous partners responsible for offering paid services related to its implementations and customizations.

The Brazilian local ERP_LC is developed by a local software house, with implementation expenses that include the acquisition of license of use and a monthly fee proportional to the number of users with access to the software. The software house has developed a dedicated optimized fast database management system that works within the standard recommended by the audit firms, not allowing direct changes to data tables. The system is remarkably light and fast, requiring relatively simple hardware configurations for smooth running.

It is noteworthy that both the SAP B1 and the Brazilian local ERP_LC have greater penetration in the local market, having hundreds of clients in the main states of the southern and southeastern Brazilian regions. Both have, as well, a consolidated network of implementing partners. Odoo is still finishing its localization stage to meet the needs imposed by the Brazilian Public Digital Bookkeeping System (SPED) project and has some of its modules deployed in dozens of companies.

3.2. Definition of the test-case for the analysis of the treatment of micro-functions in real-time

The test-case selected was a simplified purchase of inventory items, considering the entire *procure-to-pay* cycle. The selection of the procure-to-pay cycle was based upon its ubiquitous presence in different industries and based upon the importance of accounts payable environment control (Mulig and Prachyl, 2017). Very simplified tax treatment of the procurement process was assumed, and freight payments were not considered. Further, the possibility of partial delivery of purchased items or products was also not considered.

To test the role-based access functionalities, a segregation of duty (SoD) matrix was defined (Table 1). The overshadowed cells show that the same person cannot accumulate the possibility of performing both of the activities, i.e. the one described in the column and the other one, described in the row of Table 1. For example, as the creation (*letter c*) of a particular 'vendor' record (in the vendors table) and the creation of a particular purchase orders (in the respective transaction table) cannot be done within the same user profile, the cell at the interception of the 'vendors c. m. d' column and the 'purchase order c. m. d.' row is appropriately filled in.

In this particular case, suspicious purchases could be done if the same user

were able to create a new vendor record and linked it to a purchase payment order. By doing so, the fraud of deviating money to a false vendor could be facilitated. To mitigate this risk, the creation of both records cannot be done by the same person. In the implementation of the Table 1 rules, four roles/functions were created, namely # back-office, # negotiation, # fiscal, and # warehouse. The back-office function was assumed to be in charge of creation, modification, and deletion of master data. The negotiation function was deemed responsible for the creation, modification, and deletion of sales and purchase orders. The fiscal function was assumed to be in charge of the approval of orders and of adjustments in the inventory quantities. The ERP_LC functionality called 'adjustments in the inventory quantities' is to be held after an accurate *physical inventory count process*. Such adjustments generally occur when the physical inventory items are lost, damaged, or stolen. Basically, after performing 'adjustments in the inventory quantities' function, the company's system and physical inventory levels will be the same. The last role/function was held to be responsible for the moves to or from the warehouse: receiving (*incoming*) and shipping (*outgoing*).

Profile-based access control does not allow permissions to be directly associated with users. First, permissions are assigned to profiles or roles, and then each user is assigned a profile. Two different types of associations are now managed: the association between profiles and permissions; and the association between users and profiles. When a user receives a promotion reaching a managerial role, his / her profile, in general, is changed (Ferraiolo, Barkley and Kuhn, 1999; Xia et al., 2014; Shin et al., 2015). Particularly, small and medium enterprises should be prepared to avoid creating a new profile related to each new employee.

After the implementation of the profile-based access control according to the SoD matrix (Table 1), a simple example of an anomaly detection algorithm can be described as follows: in its first step, the occurrence of inventory quantity adjustments with suspicious values or frequencies will be monitored. Since there are physical barriers to ensuring that products are not misappropriated after entering inventory, the suspicious quantity adjustments could be related to the fraudulent creation of the goods receipt documents. In the algorithm, in the second step, all those responsible for entering the product in question will be identified. In the third step, if repetitive patterns can be detected with the same user receiving the same products from the same supplier; the anomaly detection algorithm can emit red alerts for further investigation. Such alerts have a high potential to assist internal auditors or supervisors in carrying out fraud-inhibiting actions.

Table 1. Segregation of duties matrix

	Clients (c,m,d)	Sales Order (c,m,d)	Approve Sales Order	Approve outgoing stock	Vendor (c,m,d)	Purchase Orders (c,m,d)	Approve Purchase Orders	Approve incoming stock	adjustments in the stock quantities
Clients (c,m,d)		XXXXX							
Sales Order (c,m,d)	XXXXX		XXXXX	XXXX					
Approve Sales Order		XXXXX							
Approve outgoing stock		XXXXX			XXXXX				XXXXX
Vendor (c,m,d)				XXXX		XXXXX			
Purchase Orders (c,m,d)					XXXXX		XXXXX	XXXX	
Approve Purchase Orders						XXXXX			
Approve incoming stock						XXXXX			XXXXX
adjustments in the stock quantities				XXXX				XXXX	

(*c =creation; m=modification; d=deletion)*

4. Modeling pillars of control of Low Complexity ERP systems

Table 2 shows the pillars of control of Low Complexity ERP readiness for continuous monitoring in SMEs. Each pillar represents a group of necessary ERP_LC functionalities to enable continuous monitoring. The first two pillars of the model - *SoD* focused on role-based access control and internal checkpoints - can be considered "low-ranging" since they do not require extra intense work to be automated, being based on existing functionalities expected to be offered by an ERP_LC. They are the two first pillars presented due to the principle established in Brennan and Teeter (2010) of prioritizing the easily automatable controls tests. The objective of both pillars is to avoid the execution of possible defective transactions, and so they represent a preventive audit effort. Considering the ERP_LC systems that have internal checkpoints as a native functionality, to have this kind of checks and balances during the transactions, in general, only requires the proper initial configuration of the ERP_LC.

The other two pillars, audit trails and integration of continuous audit software are interdependent. SMEs are not expected to pay for a customized (*add-on*) audit trail extraction. Therefore, the integration of CA software will succeed only if the ERP_LC system is able to provide an audit trail as an inbuilt or native functionality. Depending on the granularity of the process anomalies dealt with in the CA software, it can enhance a forward-looking approach that examines the validity of transactions before their final stage by comparing actual activity to the rules and the expected patterns. Based on such analyses, auditors and management can be notified beforehand about any problematic transactions and/or processes. In this convenient setting, the CA can be preventive, enabling internal auditors to actively investigate internal control exceptions as soon as they occur.

The exceptional transactions might typically be held for investigation before being released for further processing. But the complexities of the business process can contest the feasibility of this approach, and the detection of the anomalies be concretized only after the conclusion of the process, defining a detective control. So, ERP_LC with proper audit trails and enhanced open architecture can contribute to assure the effectiveness of preventive or detective controls.

Similarly, the first three pillars can be analyzed also in an integrated perspective. A finer data granularity is essential for audit trails. All details of business transactions must be processed and recorded. This granularity enables internal checkpoints and those activities subject to conflicts of interests be treated with the needed *SoD* and profile identification of the responsible person. The absence of the identification of the person accountable for the transaction annihilates the value of the audit trail.

Table 2. Modeling pillars of controls of Low Complexity ERP readiness for continuous monitoring in SMEs

	Pillar description	**Control type**
Role-based access control	Segregation of Duties (SoD) resources	preventive control
Internal Checkpoints	Resources inbuilt in ERP_LC systems implementing micro-functions checkpoints	preventive control
Audit Trail	Availability of transaction log	preventive or detective control
Level of Integration of Continuous Auditing Software	Proper interface to be integrated with CA software	preventive or detective control

5. Benchmarking and results

5.1. The background

In this section, we present the investigation as to how the four pillars presented are implemented in the three low-complexity ERP systems chosen. Each block of analysis covers a pillar of the proposed evaluation model of ERP_LC readiness for continuous auditing in SMEs, and this section is followed by the one containing a joint discussion of benchmarking results.

Even with the simplification made in the definition of the test-case for the analysis of the treatment of micro-functions, a complex step has to be taken in order to configure the three software products and to execute the data entry. The initial configuration was generic: currency, units of measurement of the products, payment deadlines, etc. Suppliers, products, and respective lists of purchase prices were registered. In the specific configuration process, after the chart of account were registered, these accounts were associated with master data of suppliers, and with the storage location. Tables with templates for automatic (pre-parameterized) postings associated with the purchase transaction were also filled out. Finally, the calendar year and the accounting period showing the cut-off, in which the test transactions would be performed, were determined.

In the tests with all three LC-ERPs, it is assumed that the person in charge of procurement verifies the need to purchase material, that purchase order is authorized, and then the purchasing sector contacts the supplier and agrees with the terms of the order. From then on, it was evaluated how each software automates the following operational activities: (i) the creation of the purchase

order, (ii) the receipt of the purchased items, and (iii) the supplier payment. The three-procedure match is an important control in purchasing. Before payment is made, there should be confirmation that the purchase is authorized (purchase order), the goods have been received (receiving report), and that the vendor has billed the company (invoice).

We define that physical inventory is the counting of the items in a company's warehouse, that increases with the receiving of goods. The logical inventory is controlled by the accounting sub-system or module that calculates and updates the inventory cost values.

Checkpoint investigation, as it is considered here, relates to an important part of the purchasing procedure. After a systemic analysis, four relevant instants are highlighted:

(1) the generation of the purchase order, which occurs when the negotiation with the chosen supplier ends and all the conditions related to the purchase are agreed upon, including also the due dates authorizations;

(2) the accounting moment of recognition of the purchase; such recognition, in accordance with accounting principles, must occur when the seller transfers the risks and rewards pertaining to the asset sold to the buyer;

(3) the entry into the physical inventory, that is, the input movement of the products purchased; and

(4) the payment to the vendor.

It is worth noting that there are different possibilities concerning the actions related to these four relevant instances. Certain purchases, for example, may have the freight as a responsibility of the buyer, wholesaler. In this case, the accounting at the wholesaler should occur as soon as the supplier issues the invoice and there is the shipment of the products, otherwise known as free on board (FOB). It is taken as a premise that at this moment there is the transmission of the rights and obligations concerning the items. It would be appropriate to use a transient account allowing the liability accounts posting, but not yet for the accounting posting related to the inventory or logical inventory. The accounting posting should be: a debit to the transient account and a credit to the supplier account. At the same time would be generated the corresponding payment invoices to the treasury. At the time of entry into physical stock, the following accounting posting would occur: a debit to an inventory account and a credit to a transient account. This accounting treatment, in addition to enabling a checkpoint in defining the definitive inventory account, also causes inventory records to always be matched with physical quantities, thus preventing errors and frauds.

5.2. Role-based access control

Except for the Brazilian local ERP_LC, the other two software products have the necessary functionality to define profiles, related to groups of functions, in order to manage the role-based access control. This is definitely a weakness of control issue, which needs to be addressed concerning the Brazilian local ERP_LC system.

The Brazilian local ERP_LC has deficiencies in dealing with the separation of duties (SoD). For instance, the movements to or from the warehouse: receiving (*incoming*) and shipping (*outgoing*) are not individually controlled. The lack of dealing separately with conflict-prone activities limits the potential use of the role-based access control.

5.3. Internal checkpoints

Relative to this topic we evaluated how the ERP software provides checkpoints through the treatment of micro-transactions in real-time and the use of transient or clearing accounts.

(i) SAP B1

Using SAP B1, the procurement process occurs conventionally in three steps. In the first step, there occurs the creation of the purchase order. In the second, the income (reception) of the product is processed (through the goods received note). In the third step, there is the creation of the document *to be paid* (A / P invoice). The first step does not impact accounting. The following activity, the receipt or income of products, comprises the movement of entry into the physical inventory and its respective logical record of the new quantity in inventory. Upon receipt of the products there will be a debit to the product inventory specific account and a credit to a transient account. It should be noted that the value of this accounting posting corresponds to the amount that must remain in the inventory account, that is, the value of the purchase net of taxes. The number of products in the logical control of inventory is also updated in this action and calculated is the new unitary cost of the product. In the third step, there is the creation of the document *to pay* (A/P Invoice). This is an internal purchase document that mirrors the invoice received from the supplier.

While most countries' authorities usually require an invoice document in order to charge the customer and also declare VAT to be collected to the order to cash process, Brazil works according to a different approach. In almost all business transactions the electronic invoice (*Nota Fiscal)* document is required. Whatever goods the company moves to the third party; an electronic invoice is also required. The cargo transportation is required to be made with a paper copy of the invoice, called *Danfe*. The invoice has an official form and layout given by the government, which includes all data related to sender taxpayer,

customer, goods, unit and total price, tax base and tax amounts, payment terms, forwarding agent and so on.

For instance, Table 3 shows a possible third step accounting postings considering Brazilian *ICMS* tax, which is like Sales tax.

Table 3. Possible accounting postings associated with the creation of A/P invoice in SAP B1

Dr: Transient account - that was credited in the receipt or income of products Dr: ICMS tax paid Cr: Vendor

(ii) Odoo Software

Using Odoo software, the Purchasing Manager / Buyer creates a purchase order. This action also creates an incoming shipment order with a 'waiting' *status* and a draft invoice.

In the treasury or cash management department, the Accounts Payable clerk validates the Draft invoice, which is transformed into an Invoice with an 'open' status. At this point in time, a preliminary logical entry is made through the following accounting posting: a temporary/clearing account is debited and the supplier account is credited with the value of the purchase.

During the inbound delivery process, the warehouse clerk will process the physical entry that occurs only if the purchase order data matches the products received with the accompanying invoices. The action is meant to change the Incoming Shipment order status to 'received/available', as shown on the process-based approach (PBA) diagram of Fig. 1. The consequences of this action will be: (i) the definite account posting, comprising: a debit to the product inventory account and a credit to the transient/clearing account; (ii) the calculation of product (inventory item) new value, using weighted average cost method; and (iii) logical record of the new quantity in inventory.

The Accounts Payable clerk pays, at the invoice due date, the A/P invoice; after checking if the status of the incoming shipment order is 'received'. As a payment split, the A/P invoice status will change from 'open' to 'paid', and the following accounting posting will be generated: a debit to the supplier account and a credit to the bank account.

It should be emphasized that all accounting entries must still be validated by accounting and only then will this be recorded in the general ledger.

(iii) Brazilian local ERP_LC

Using the Brazilian local ERP_LC, the Purchasing Manager/Buyer, in the Purchasing module creates a purchase order that will have a pending status until

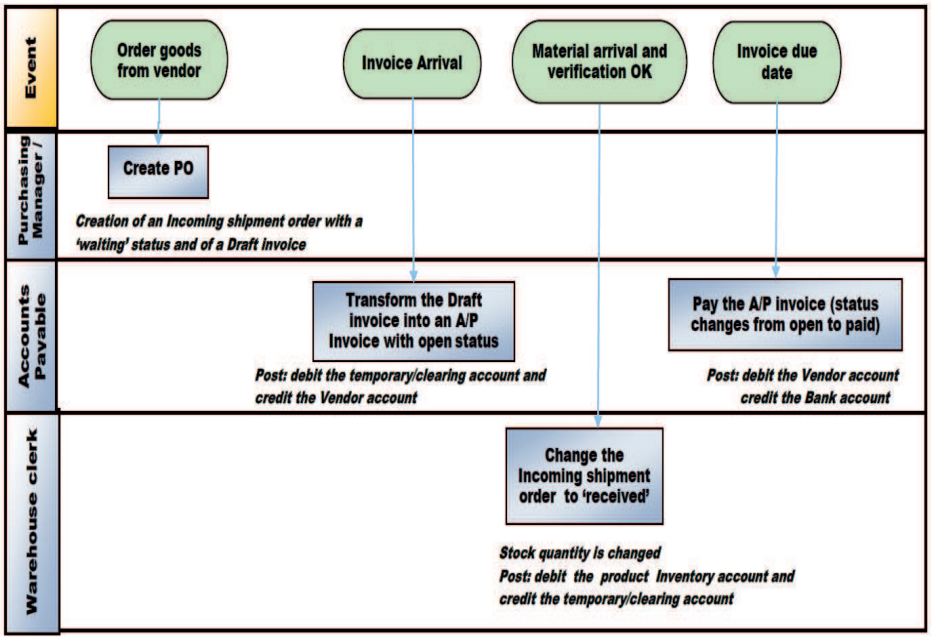

Figure 1. Purchase PBA in Odoo software

the products arrive. After the arrival of the products, the person responsible for the logical entry will originate the 'Entry record' in the same Purchasing module. It is worth noting that the execution of just one action triggers many activities:

- the purchase order obtains the newly 'attained' status,
- an accounting posting: a debit the inventory account and a credit to the supplier account;
- the creation of the documents related to the A/P invoice in the Treasury module, with a 'ready to be paid' status;
- the calculation of product new cost value; and
- the logical record of the new quantity in inventory.

The lack of the one-to-one relationship between action and activity triggered causes problems. As this action is done in the purchasing module, it can be assumed that it is carried out by a purchasing clerk. Assuming that is not his function to verify the quantity physically received, as a result of the merging of activities associated with this one action, no one can be blamed for inventory entries that could be related to fraudulent acts.

After the 'Entry record' creation, in the Treasury module, it is possible to carry out the write-off of documents to be paid. The impact of this action will

be the following accounts posting, a debit to the supplier account, and a credit to the bank account; and the change of the status of the A/P invoice to 'cleared'.

5.4. Comparison of the micro activities of the purchase process and of the internal checkpoints

Both in SAP B1 and in Odoo, the micro-functions are synchronized with the use of transient accounts. In the SAP B1, the physical entry in the inventory triggers the logical entry with the counterpart in the temporary/clearing account, associated with physical reception. This account will be verified and zeroed out in the creation of the A/P invoices. In the use of the Odoo, there is also a checkpoint, however, comparing it with the SAP B1's, the order of the internal check is reversed: first, the treasury validates the document to be paid, by crediting the supplier account and debiting the temporary/clearing account. Subsequently, at the physical receipt of the merchandise, there is the verification and the zeroing out of the temporary/clearing account. Although the synchronization in the SAP B1 determines that first there is the entry into the inventory and then the generation of the document to be paid; and the synchronization in Odoo reverses this order, what is relevant is that in both systems there is the introduction of checkpoints.

In the Brazilian local ERP_LC, there is no checkpoint. Actually, there is no separation between the treatment of the entry of products into the physical inventory, the approval of incoming inventory activity, and the other activities: accounting posting and financial processing of A/P invoice.

5.4.1. Audit Trail

(i) SAP B1

The audit trails provided by SAP Business One (*version 8.8 Patch 18*) can be easily obtained through the access log option or through the change log option. As for the change log option, the number of old instances of an object, for example, a bank account, which one wishes to keep, can be parameterized. As a result, in addition to the current record, a configured number of records of the same bank account with different previous values will also be stored. The penultimate record brings the bank account data prior to the last change, linked to the activities or micro-operations that caused such change.

It is also possible to notice how many users were simultaneously connected to the system, and even though many of them viewed the same object, it is possible to trace which user actually changed it. The concept of objects includes master data, such as: business partners, products, bank accounts, etc. and also documents, such as: sales orders, shipping orders; purchase orders, etc. In total, the SAP B1 treats 132 types of objects, each of them stored in at least one table with the creation date and responsible user identification.

(ii) Odoo

Version 7 of Odoo did not have the audit trail as a default functionality. However, an extra tool, known as the audit trail tool, allows users with a system administrator profile to obtain an audit trail called "log users operation". It is possible to trace the users who have performed creation, reading, writing, and deletion on each object.

By the number of downloads of this extra tool, it can be inferred that it is not widely used by the community, which can make it difficult for the correction of its possible errors and bugs, as well as the development of new audit trail features.

(iii) Brazilian local ERP_LC

The local software can also identify the users who were connected to the system and the activities performed by them. It must be emphasized that this software's deficiency in dealing with the separation of activities damages the potential use of its audit trail. The identification of the time and of the user is attached to object creation, modification, or deletion. But if the action is a change, it is not known what has been modified. If two users have done the same action on an object, a purchase order, for example, it may not be possible to detect which change each user made.

5.4.2. Level of integration of continuous auditing software

(i) SAP B1

This ERP_LC has some built-in audit features. Therefore, it can be said that a part of the continuous audit software is embedded in the ERP_LC, so it can be classified as EAM hybrid.

As previously discussed, SAP B1 allows for the monitoring of modifications to objects. The audit trail also includes accounting inventory postings related to receipt of goods when materials enter the warehouse and to the outgoing movements, when materials leave the warehouse. All inventory transactions, whether they are incoming, like those from Purchasing and from Production Control modules, or are outgoing, as those from Sales module; will be recorded in the audit trail. If there are manual inventory transaction entries into the SAP B1, the different quantity value, appearing in the Warehouse Control module in relation to the Accounting module, can be tracked in detail with this tool. There are also SAP B1 add-ons and applications, in a hybrid MCL model, that increase the possibilities of continuous monitoring. These applications explore the open architecture components made available by the SAP B1 software development kit. When considering the compliance of the required criteria for add-ons, applications developed by the third parties are certified by SAP and made available to users in a proper security standard. Commercial audit packages (ACL, IDEA or Caseware analytics) can also be used to process the data obtained by specific data extraction processes.

(ii) Odoo

Odoo version 7 did not offer integration with continuous audit software options. However, considering all the low complexity ERP systems analyzed, in Odoo, which is open-sourced, the development of continuous auditing software can be done easier in an EAM model. Its open-sourced development allows for programming in the same language, and for access to the same databases, which can configure continuous auditing software in a typically EAM architecture. In a less integrated manner, generalized audit packages (ACL, IDEA or Caseware analytics) can also be used, post-processing the data obtained by specific data extraction applications.

(iii) Brazilian local ERP_LC

During this research, there was no possibility to integrate the national ERP with continuous audit software in an EAM model. The software development process is completely closed, the software having been developed up for a database management system dedicated to it. Until its software house decides to provide continuous audit software, or to provide a specific interface to allow data extraction with generalized audit packages, the possibility of using software to further process transaction data will be practically non-existent.

6. Discussion

This study verified that both SAP B1 and Odoo met the demands of the *role-based access control* and of *internal checkpoints,* being the two first pillars of the ERP_LC readiness evaluation model. And concerning audit trails, SAP B1 made this resource available in the most comprehensive way. Odoo addresses auditing trails in an extra module, so its functionalities could not be completely explored and understood. Nevertheless, as an open-sourced software, Odoo has the potential to provide detailed tracks. The fourth pillar requirements, which concerns the integration of continuous audit software, were satisfactorily fulfilled only through SAP B1. Odoo, as an open-source software, has the potential for full integration of continuous audit software, however, these possibilities of implementation could not be tested.

The model's ability to distinguish between the low complexity ERP's functionalities and features can contribute to the perception of its validity. The proposition of this model with the addition of assessment criteria in the low complexity ERP selection process can be considered the main contribution of this paper. There is also another important contribution made by the present paper, consisting in the description of test-case selection process, allowing the proper analysis of the micro-functions.

In the same vein, it is important to note that the relevance as to the investigation of the possibilities of implementation of internal control in a developing country is propelled by the notorious issues of frauds and corruptions worldwide, this aspect being also supported by Foreign Corrupt Practices Act (FCPA) and

the Sarbanes Oxley Act (SOX) for the traded and larger organization. This also remains fully valid when the control environment of the SMEs is being discussed. Regarding small businesses, the importance of the respective discussion can be justified by their pronounced role in the Brazilian economy and in the global scene, particularly so with respect to job creation (Guimaraes, Carvalho and Paixão, 2018; Gupta, Gregoriou and Healy, 2015).

When continuous auditing is considered a critical real-time monitoring tool of transactions, SMEs managers and other stakeholders will demand that the evaluation of ERP_LC candidates (Illa, Franch and Pastor, 2000; Deep et al., 2008; Asgar and King, 2016) consider the functionalities presented in the four pillar model and also the openness of the ERP_LC architecture, which could be assessed as per Table 4, allowing its smooth integration with the CA software, this being considered to be a more technical than a functional evaluation.

Table 4. Assessment criteria added

Business Area:	Accessment Criteria Added	None Marginal Medium Strong Optimal 1 2 3 4 5
production planning	.....	
	Internal Checkpoints in micro-functions	☐☐☐☐☐
	.....	
HR	.....	
	Internal Checkpoints in micro-functions	☐☐☐☐☐
	.....	
purchase	.....	
	Internal Checkpoints in specific micro-functions	☐☐☐☐☐
	.....	
sales and marketing	.....	
	Internal Checkpoints in specific micro-functions	☐☐☐☐☐
	.....	
finance	.....	
	Internal Checkpoints in specific micro-functions	☐☐☐☐☐
	Using clearing or transient accounts	☐☐☐☐☐
	.....	
none (*system as a whole*)	.....	
	Role-Based Access Control	☐☐☐☐☐
	Audit Trail	☐☐☐☐☐
	Openness(integration with CA software)	☐☐☐☐☐
	.....	

As a preconception, certain inferiority of the Brazilian local ERP_LC was

expected in presenting functionalities and features meant to enhance continuous monitoring, based on the fact that Brazilian organizational culture tends to attribute comparatively lesser value to internal controls. According to Alles et al. (2006b), in comparison to The Netherlands, England and the U.S., the percentage of audit professionals per capita in Brazil is extremely low.

Notwithstanding the above reservations, the complete inadequacy of Brazilian local ERP_LC was an unexpected result. There are many negative outcomes from the fact that the Brazilian local ERP_LC does not treat separately the activities of approving incoming inventory items but condenses all the following actions in a macro activity: # accounting posting, # A/P invoice financial processing, # calculation of product (inventory item) new value, and # the logical record of the new quantity in inventory. First of all, it was not possible for the implementation of the profile-based access control according to the SoD matrix shown in Table 1. Also, it was not possible to implement internal checkpoints through the treatment of micro-functions in real-time, using transient accounts.

Overall, the current understanding of the concepts, related to the efforts to implement CA in small business with ERP_LC has advanced. A potential shortcoming could be the project finance of open architecture resources that brings serious restrictions to the integration with continuous audit software in the SME environment. The local software having no adherence to the ERP_LC readiness for continuous monitoring pillars implies the inadequacy of its usage by SMEs that are looking for the improvement of internal control.

7. Concluding remarks

This article intends to make a step forward in the literature on what are the basic pillars that define functionalities and features required of the readiness of low complexity ERP systems to feasibly implement the continuous data auditing and continuous monitoring in the SMEs. In order to attain this objective, an extensive underpinning literature review of such basic resources was done. Based on our findings, we conclude that the four pillars of the evaluation model are segregation of duties (*SoD*) with role-based access control; internal checkpoints; audit trails; and the possibilities of integration of the continuous data auditing and process monitoring software.

It is noteworthy that the pillars of *SoD* in conjunction with the role-based access and inclusion of internal checkpoints effectively supports the preventive controls. At the same time, the audit trails and integration of continuous audit software contribute to assuring the preventive, detective or even corrective controls, depending upon small business processes and internal control architecture.

Depending on the conjecture of the control environment for systems implementation, without the proper interface to integrate CA software as complementary solutions, the efforts to implement CA in small business with ERP_LC

can be unproductive. Thus, proper audit trails and enhanced open architecture can contribute to ensuring the effectiveness of preventive or detective controls.

The application of the assessment model in the three ERP_LC systems: SAP B1, Odoo and Brazilian local ERP_LC was not intentionally made to compare the systems but rather to explore their specificities. The practical application of the concepts contained in the pillars allowed for their definition with greater clarity.

The model's ability to distinguish between low complexity ERP's functionalities and features reveals that it brought an important contribution to the study of low complexity ERP's readiness for continuous monitoring in SMEs internal auditing processes. Thus, this study has contributed to bridging the gap between research and practice on issues related to the readiness of low complexity ERP in view of continuous monitoring in SMEs, enabling knowledge to be shared effectively among academia, practitioners, and policy makers.

Finally, in order to speculate on the future directions of research we encourage investigations on the operational aspects of the ERP_LC systems with a broader coverage mixing it with the impact of the different cultures for analysis. We also suggest that interpretive research be done in regard to audit trails and anomaly detection in order to expand on the thematic analysis.

References

Alaküla, M. L. and Matulevičius, R. (2015, November) An experience report of improving business process compliance using security risk-oriented patterns. In: *IFIP Working Conference on The Practice of Enterprise Modeling*, 271-285. Springer, Cham.

Alles, M. G., Brennan, G., Kogan, A. and Vasarhelyi, M. A. (2006a) Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. *International Journal of Accounting Information Systems*, **7**(2), 137-161.

Alles, M. G., Tostes, F., Vasarhelyi, M. A. and Riccio, E. L. (2006b) Continuous auditing: the USA experience and considerations for its implementation in Brazil. *JISTEM - Journal of Information Systems and Technology Management*, **3**(2), 211-224.

Alles, M. G., Kogan, A. and Vasarhelyi, M. A. (2008) Putting continuous auditing theory into practice: Lessons from two pilot implementations. *Journal of Information Systems*, **22**(2), 195-214.

Antunes, M. T. P., Imoniana, J. O., Formigoni, H. and Alves, A. S. (2010) Preparedness of ERP systems to create intangible managerial accounting information: evidence from Brazil. *International Journal of Economics and Accounting*, **1** (4), 375-390.

Bagheri, A. and Hjorth, P. (2005) Monitoring for sustainable develop-

ment: Systemic framework. *Int. J. of Sustainable Development*, **8**(4), 280-301.

Baker, W. E., Grinstein, A. and Harmancioglu, N. (2016) Whose innovation performance benefits more from external networks: entrepreneurial or conservative firms? *Journal of Product Innovation Management*, **33**(1), 104-120.

Batra, S., Sharma, S., Dixit, M. R., Vohra, N. and Gupta, V. K. (2015) Performance implications of industry appropriability for manufacturing SMEs. *Journal of Manufacturing Technology Management*, **26**(5), 660–677.

Best, P. J., Rikhardsson, P. and Toleman, M. (2009) Continuous fraud detection in enterprise systems through audit trail analysis. *Journal of Digital Forensics, Security and Law*, **4**(1), 1-6.

Bierstaker, J., Janvrin, D. and Lowe, D. J. (2014) What factors influence auditors' use of computer-assisted audit techniques? *Advances in Accounting*, **30**(1), 67-74.

Blessing, L. T. M. (1994) A process-based approach to computer-support engineering design. Dissertation, University of Twente, ISBN 0.9523504.0.8, Enschede. 369 pp.

Brennan, G. and Teeter, R. (2010) Aiding the Audit: Using the IT Audit as a Springboard for Continuous Controls Monitoring. Available at SSRN: https://ssrn.com/abstract=1668743 or http://dx.doi.org/10.2139/ssrn.1668743

Brown, C. E., Wong, J. A. and Baldwin, A. A. (2007) A review and analysis of the existing research streams in continuous auditing. *Journal of Emerging Technologies in Accounting*, **4**(1), 1-28.

Bumgarner, N. and Vasarhelyi, M. (2015) Auditing—A New View. *Audit analytics* **3**(1), 2015.

Cahen, F. R., Lahiri, S. and Borini, F. M. (2016) Managerial perceptions of barriers to internationalization: An examination of Brazil's new technology-based firms. *Journal of Business Research*, **69**(6), 1973-1979.

Clausing, D. and Holmes, M. (2010) Technology readiness. *Research-Technology Management*, **53**(4), 52-59.

COSO - Committee of Sponsoring Organizations of the Treadway Commission (2013). Internal Control-Integrated Framework.

Coyte, R., Ricceri, F. and Guthrie, J. (2012) The management of knowledge resources in SMEs: an Australian case study. *Journal of Knowledge Management*, **16**(5), 789-807.

Daniels, B. W., Ellis, Y. and Gupta, R. D. (2013) Accounting educators and practitioners' perspectives on fraud and forensic topics in the accounting curriculum. *Journal of Legal, Ethical and Regulatory Issues*, **16**(2), 93.

Davidson, B. I., Desai, N. K. and Gerard, G. J. (2013) The effect of continuous auditing on the relationship between internal audit sourcing

and the external auditor's reliance on the internal audit function. *Journal of Information Systems*, **27**(1), 41-59.

Debreceny, R., Gray, G. L., Jun-Jin Ng, J., Lee, K. S.-P. and Yau, W.-F. (2005) Embedded audit modules in enterprise resource planning systems: Implementation and functionality. *Journal of Information Systems*, **19**(2), 7–27.

Deep, A., Guttridge, P., Dani, S. and Burns, N. (2008) Investigating factors affecting ERP selection in made-to-order SME sector. *Journal of Manufacturing Technology Management*, **19**(4), 430-446. https://doi.org/10.1108/17410380810869905

Denning, D. E. (1987) An Intrusion-Detection Model. *IEEE Transactions on Software Engineering*, **13**(2), 222-232.

DeZoort, F. T. and Harrison, P. D. (2018) Understanding auditors' sense of responsibility for detecting fraud within organizations. *Journal of Business Ethics*, **149**(4), 857-874.

Eulerich, M. and Kalinichenko, A. (2018) The current state and future directions of continuous auditing research: An analysis of the existing literature. *Journal of Information Systems*, **32**(3), 31-51.

Ferraiolo, D. F., Barkley, J. F. and Kuhn, D. R. (1999) A role-based access control model and reference implementation within a corporate intranet. *ACM Transactions on Information and System Security*, **2**(1), 34-64.

Gershberg, T. (2016) Log4Audit: the application of logging in auditing and management. Doctoral dissertation, Rutgers University-Graduate School-Newark. Available at https://rucore.libraries.rutgers.edu/rutgers-lib/51554/PDF/1/play/

Gómez-López, M. T., Gasca, R. M. and Pérez-Álvarez, J. M. (2015). Compliance validation and diagnosis of business data constraints in business processes at runtime. *Information Systems*, 48, 26-43.

Gonzalez, G. C., Sharma, P. N. and Galletta, D. (2012) Factors influencing the planned adoption of continuous monitoring technology. *Journal of Information Systems*, **26**(2), 53-69.

Groomer, S. M. and Murthy, U. S. (1989) Continuous auditing of database applications: An embedded audit module approach. *Journal of Information Systems*, **3**(2), 53-67.

Guimarães, A. B. S., Carvalho, K. C. M. and Paixão, L. A. R. (2018) Micro, pequenas e médias empresas: conceitos e estatísticas. *Revista Radar: tecnologia, produção e comércio exterior*, **1**(55), 21-26.

Gupta, H., Aye, K. T., Balakrishnan, R., Rajagopal, S. and Nguwi, Y. Y. (2014) Formulating, implementing and evaluating ERP in small and medium scale industries. *International Journal*, **3**(6).

Gupta, J., Gregoriou, A. and Healy, J. (2015) Forecasting bankruptcy for SMEs using hazard function: To what extent does size matter? *Review of Quantitative Finance and Accounting*, **45**(4), 845-869.

Haddara, M. and Zach, O. (2012) ERP systems in SMEs: An extended

literature review. *International Journal of Information Science*, **2**(6), 106-116.

Haynes, R. and Li, C. (2016) Continuous audit and enterprise resource planning systems: A case study of ERP rollouts in the Houston, TX oil and gas industries. *Journal of Emerging Technologies in Accounting*, **13**(1), 171-179. https://doi.org/10.2308/jeta-51446

Hevner, A. and Chatterjee, S. (2010) Design science research in information systems. In: *Design Research in Information Systems*. Springer, Boston, MA, 9-22.

Illa, X. B., Franch, X. and Pastor, J. A. (2000) Formalising ERP selection criteria. In: *Tenth International Workshop on Software Specification and Design. IWSSD-10 2000*. IEEE, 115-122.

Imoniana, J.O., Perera, L. C. J., Lima, F. G. and Antunes, M. T. P. (2011) The dialectic of Control Culture in SMEs: A Case study. *International Journal of Business Strategy*, **11**(2), 39-48.

Imoniana, J. O., Feitas, E. C. D. and Perera, L. C. J. (2016) Assessment of internal control systems to curb corporate fraud-evidence from Brazil. *African Journal of Accounting, Auditing and Finance* **5** (1), 1-24.

Jans, M., Alles, M. G. and Vasarhelyi, M. A. (2014) A field study on the use of process mining of event logs as an analytical procedure in auditing. *The Accounting Review*, **89**(5), 1751-1773.

Jituri, S., Fleck, B. and Ahmad, R. (2018) A Methodology to Satisfy Key Performance Indicators for Successful ERP Implementation in Small and Medium Enterprises. *International Journal of Innovation, Management and Technology*, **9**(2).

Kim, Y. and Kogan, A. (2014) Development of an anomaly detection model for a bank's transitory account system. *Journal of Information Systems*, **28**(1), 145–165.

Kobelsky, K. W. (2014) Conceptual Model for Segregation of Duties: Integrating Theory and Practice for Manual and IT-Supported Procedures. *International Journal of Accounting Information Systems*, **15**(1), 304–322.

Kogan, A., Alles, M. G., Vasarhelyi, M. A. and Wu, J. (2010) *Analytical Procedures for Continuous Data Level Auditing: Continuity Equations 1.* Available at http://raw.rutgers.edu/docs/Innovations/Continuity%20Equations.pdf

Kogan, A., Alles, M. G., Vasarhelyi, M. A. and Wu, J. (2014) Design and evaluation of a continuous data level auditing system. *Auditing: A Journal of Practice & Theory*, **33**(4), 221-245.

Kuhn, J. R. and Sutton, S. G. (2006) Learning from WorldCom: Implications for fraud detection through continuous assurance. *Journal of Emerging Technologies in Accounting*, **3**(1), 61-80.

Kuhn, J. R. and Sutton, S. G. (2010) Continuous Auditing in ERP System Environments: The Current State and Future Directions. *Journal of Information Systems*, **24**(1), 91–112.

Lee, C. H., Kim, Y. H. and Rhee, P. K. (2001) Web personalization

expert with combining collaborative filtering and association rule mining techniques. *Expert Systems with Applications*, **21**(3), 131-137.

Lenz, R. and Hahn, U. (2015) A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities. *Managerial Auditing Journal*, **30**(1), 5-33.

Li, S. H., Huang, S. M. and Lin, Y. C. G. (2007) Developing a continuous auditing assistance system based on information process models. *Journal of Computer Information Systems*, **48**(1), 2-13.

Li, H., Dai, J., Gershberg, T. and Vasarhelyi, M. A. (2018) Understanding usage and value of audit analytics for internal auditors: An organizational approach. *International Journal of Accounting Information Systems*, 28, 59-76.

Lu, J. W. and Beamish, P. W. (2006) SME internationalization and performance: Growth vs. profitability. *Journal of International Entrepreneurship*, **4**(1), 27–48.

Ly, L. T., Maggi, F. M., Montali, M., Rinderle-Ma, S. and van der Aalst, W. M. (2015) Compliance monitoring in business processes: Functionalities, application, and tool-support. *Information Systems*, 54, 209-234.

Manolova, T. S., Manev, I. M. and Gyoshev, B. S. (2010) In good company: The role of personal and inter-firm networks for new-venture internationalization in a transition economy. *Journal of World Business*, **45**(3), 257–265.

Mokhitli, M. and Kyobe, M. (2019) Examining factors that impede internal auditors from leveraging information technology for continuous auditing. In: *Proceedings of Conference on Information, Communications, Technology and Society (ICTAS)*, Durban, South Africa, 1-6.

Muhrtala, T. O. and Ogundeji, M. (2013) Computerized accounting information systems and perceived security threats in developing economies: The Nigerian case. *Universal Journal of Accounting and Finance*, **1**(1), 9-18.

Mulig, L. and Prachyl, C. L. (2017) Identifying Red Flags in an Accounts Payable Environment: The Importance of Controls in the Detection of Fraudulent Activity. *Journal of Forensic & Investigative Accounting,* **9**(3), 941-952.

Munro, D. (2013) *A Guide to SME Financing*. Springer.

OSI (2016) *Open Source Initiative*. Available at https://opensource.org/osd

Poba-Nzaou, P. and Raymond, L. (2011) Managing ERP system risk in SMEs: A multiple case study. *Journal of Information Technology*, **26**(3), 170-192.

Powell, D., Riezebos, J. and Strandhagen, J. O. (2013) Lean production and ERP systems in small-and medium-sized enterprises: ERP support for pull production. *International Journal of Production Research*, **51**(2), 395-409.

Rikhardsson, P. and Dull, R. (2016) An exploratory study of the adop-

tion, application and impacts of continuous auditing technologies in small businesses. *International Journal of Accounting Information Systems*, 20, 26-37.

Rikhardsson, P., Singh, K. and Best, P. (2019) Exploring Continuous Auditing Solutions and Internal Auditing: A Research Note. *Journal of Accounting and Management Information Systems*, **18**(4), 614-639. https://doi.org/10.24818/jamis.2019.04006

Santos, L. M., Silva, G. M. and Neves, J. A. B. (2011) Risk of Survival of Commercial Micro and Small Enterprises. *Revista de Contabilidade e Organizações*, **5**(11), 107-124.

Schultz, M. (2013) Enriching process models for business process compliance checking in ERP environments. In: *Proceedings of International Conference on Design Science Research in Information Systems*. Springer, Berlin.

Shin, I. H., Lee, M. G. and Park, W. (2013) Implementation of the continuous auditing system in the ERP-based environment. *Managerial Auditing Journal*, **28**(7), 592–627.

Shin, M. S., Jeon, H. S., Ju, Y. W., Lee, B. J. and Jeong, S. P. (2015) Constructing RBAC based security model in u-healthcare service platform. *The Scientific World Journal*, 2015.

Singh, K. H. et al. (2011) Proactive fraud detection in enterprise systems. In: *Proceedings of the 2nd International Conference on Business and Information: Steering Excellence of Business Knowledge*. University of Kelaniya, Faculty of Commerce and Management Studies.

Singh, K. H. et al. (2013). Automating vendor fraud detection in enterprise systems. *The Journal of Digital Forensics, Security and Law*, **8**(2), 7-28.

Singh, K. H., Best, P. J., Bojilov, M. and Blunt, C. (2014) Continuous Auditing and Continuous Monitoring in ERP Environments: Case Studies of Application Implementations. *Journal of Information Systems*, **28**(1), 287–310.

Valarini, E. and Pohlmann, M. (2019) Organizational crime and corruption in Brazil; a case study of the "Operation Carwash" court records. *International Journal of Law, Crime and Justice*, 59, 1-15.

Van der Aalst, W., Van Hee, K., Van der Werf, J. M., Kumar, A. and Verdonk, M. (2011) Conceptual model for online auditing. *Decision Support Systems*, **50**(3), 636-647.

Vasarhelyi, M. A., Alles, M. A. and Kogan A. (2004) Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting*, **1**(1), 1–21.

Vasarhelyi, M. A., Alles, M. G., Kuenkaikaew, S. and Littley, J. (2012) The acceptance and adoption of continuous auditing by internal auditors: A micro analysis. *International Journal of Accounting Information Systems*, **13**(3), 267–281.

Vaz, P. V. C. and Espejo, M. M. S. B. (2015) From text to context: management accounting use in micro and small companies under the the-

oretical perspective of Bakhtin. *Revista de Contabilidade e Organizações*, **9**(24), 31-41.

Veasey, T. J. and Dodson, S. J. (2014) Anomaly detection in application performance monitoring data. *International Journal of Machine Learning and Computing*, **4**(2), 120.

Wang, J., Shan, Z., Gupta, M. and Rao, H. R. (2019) A Longitudinal Study of Unauthorized Access Attempts on Information Systems: The Role of Opportunity Contexts. *MIS Quarterly*, **43**(2).

Wolter, C., Miseldine, P. and Meinel, C. (2009) Verification of Business Process Entailment Constraints Using SPIN. In: F. Massacci, S. T. Redwine Jr. and N. Zannone (eds.) *ESSoS 2009* - **LNCS 5429**, Springer, 1-15.

Xia, H. et al. (2014) Role Refinement in Access Control: Model and Analysis. *INFORMS Journal on Computing*, **26**(4), 866-884.

Zadeh, A. H., Akinyemi, B. A., Jeyaraj, A. and Zolbanin, H. M. (2018) Cloud ERP Systems for Small-and-Medium Enterprises: A Case Study in the Food Industry. *Journal of Cases on Information Technology*, **20**(4), 53-70.