Received: 20 February 2020 | Revised: 13 May 2020 | Accepted: 1 June 2020

DOI: 10.1002/bse.2558

RESEARCH ARTICLE

Business Strategy and the Environment

WILEY

Continuous auditing and data mining for strategic risk control and anticorruption: Creating "fair" value in the digital age

Andrea Cardoni[1] | Evgeniia Kiseleva[1] | Francesco De Luca[2]

[1]Department of Economics, University of Perugia, Via Alessandro Pascoli, 20, Perugia, Italy

[2]Department of Business Administration and Management, University "G. DAnnunzio" at Chieti-Pescara, Pescara, Italy

Correspondence
Andrea Cardoni, Department of Economics, University of Perugia, Via Alessandro Pascoli, 20, Perugia, PG 06123, Italy.
Email: andrea.cardoni@unipg.it

Abstract

This paper aims to bridge a gap in the literature by investigating a continuous audit case for anticorruption. The evolution of technology can offer valuable opportunities to integrate legality checks and business processes that are consistent with the growing call to fight corruption at the institutional level. Since the last decade, researchers have proposed conceptual frameworks demonstrating the visible advantages of continuous auditing and data mining, but significant difficulties still exist in practice. This process has been implemented in only a few cases, and the lack of empirical studies implies a need for additional research on this topic.

To fill this gap, we adopt the framework proposed by Chan and Vasarhelyi (2011) and identify success factors for the implementation of continuous auditing. For the analysis, we use the research methodology of a single case study and focus on the Italian company Acciai Speciali Terni Spa (AST), the only steelwork company in Europe that has been ISO 37001 certified. This study demonstrates the practical impact of continuous auditing and data mining on strategic risk control by empirically testing the Chan and Vasarhelyi (2011) framework for the specific issue of anticorruption. The results show that effective continuous auditing is centered on an integrative and change management approach and that strategic vision, risk mapping, and a no-corruption culture are among the most influential factors. The AST case demonstrates that technology is currently essential for supporting strategic risk control but only if it is integrated with consistent growth in organizational and managerial capabilities.

KEYWORDS

anticorruption, continuous auditing, data mining, strategic risk control

1 | INTRODUCTION

Corruption is one of the most urgent topics at present. The latest estimates suggest that the cost of corruption across the EU is a loss to GDP of €179–950 billion per year (The Greens/EFA in the EU Parliament, 2018). Almost 20% of organizations worldwide report receiving at least one bribery payment request during regulatory or utility transactions (UN Global Compact, 2019). Corruption has detrimental consequences; organizations lose approximately 5% of their annual revenues to fraud, and corruption also undermines confidence and trust among various stakeholders (Association of Certified Fraud Examiners, 2018). Nevertheless, companies are unwilling or unable to undertake efficient active measures against corruption. The greatest amount of loss due to corruption is still detected by passive methods, such as notifications from law enforcement, confessions, or accidents (Association of Certified Fraud Examiners, 2018).

Internal audit has great potential to identify corrupt actions (Lombardi, Trequattrini, Cuozzo, & Cano-Rubio, 2019). Auditors have

a unique position within firms as public interest representatives who monitor and report on an organization's compliance (Jeppesen, 2019). Internal auditors are independent and have knowledge and insight, assuring a high likelihood of fraud detection. However, in practice, only 15% of corrupt actions are detected by internal auditors (Association of Certified Fraud Examiners, 2018).

The low effectiveness of the internal audit function may be explained by the obsolete tools that it uses. The current sampling methods and periodic audits with "ex ante" approvals are becoming irrelevant in the era of ongoing big data accumulation and analysis and instant decision making. Digitalization, Industry 4.0, the Internet of Things, and cloud computing are the first challenges for internal auditors in 2020 (KPMG, 2018). Additional challenges include globalization with expansion into new markets, dealings with third parties and business acquisitions, emerging tight regulatory norms in the sphere of data security and compliance risk, the rapid social media reaction to corrupt actions, and growing pressure from key stakeholders (KPMG, 2018).

The solution to these modern challenges may be the continuous audit paradigm formulated by Groomer and Murthy (2018) and Vasarhelyi and Halper (1991) (Chan & Vasarhelyi, 2011). Continuous audit differs from the traditional approach in terms of its frequency, focus on automated processes, and unique concept of exception analysis (Vasarhelyi, Alles, & Williams, 2010; Vasarhelyi & Halper, 1991), which enhances the relevance and timeliness of the audit results (Chiu, Liu, & Vasarhelyi, 2014).

Although continuous auditing is very advantageous, its usage is still infrequent (Cipriano, Pereira, Almeida, & da Silva, 2019). Companies are not ready to actively adopt it because the concept remains vague. Researchers have proposed theoretical principles, conceptual frameworks, and enabling technologies, but experimental and empirical studies are lacking (Chiu et al., 2014; Kogan, Sudit, & Vasarhelyi, 2018; , 2000), as are studies that expand upon the basic elements (Bumgarner & Vasarhelyi, 2018). Moreover, the link between continuous audits and corruption is unclear and requires additional research (Jeppesen, 2019).

Our study aims to bridge this gap in the literature by providing an empirical study of continuous audit cases for anticorruption. We adapt Chan and Vasarhelyi's (2011) most comprehensive continuous audit model to study anticorruption and identify success factors for its implementation. To do so, we use the research methodology of a single case study focusing on the Italian company Acciai Speciali Terni Spa (AST), which saved more than €100 million with the help of the continuous audit technique for anticorruption.

The remainder of this paper is organized as follows. Section 2 describes the traditional and continuous audit approaches to anticorruption in the context of the evolution of modern technology. We then describe the methodology in Section 3. In Section 4, we present Chan and Vasarhelyi's (2011) continuous audit model adapted for anticorruption and support it with the practical example of AST in Section 5. Section 6 discusses the success factors that allowed AST to make the model efficient. The last section provides conclusions and suggestions for future research.

2 | LITERATURE REVIEW

2.1 | The evolution of auditing approaches to anticorruption

A company's control functions (i.e., internal audit or internal control system functions) play the main role in its corruption prevention and transparency (Jeppesen, 2019; Lombardi et al., 2019). Thus, the effectiveness of anticorruption efforts largely relies on having an effective audit model.

Under the traditional audit paradigm, auditors conduct risk evaluations for different procedures and choose a sample of data to investigate corruption on a material basis (Wells, 2003). Manual testing exists at all stages of auditing, from planning to reporting (Vasarhelyi, Alles, Kuenkaikaew, & Littley, 2012). However, the sample approach bears the risk of missing data about corruption activities in big data sets, and yearly or quarterly manual audits can have too large a lag between corrupt actions and ex ante control, which is unacceptable in the current economy of instant decision making (KPMG, 2018; Vasarhelyi et al., 2010, p. 20). Moreover, new technologies lead to new types of fraud and corruption schemes that are not detectable by traditional tools (Cipriano et al., 2019).

More frequent or continuous audits are becoming increasingly important. The objectives of such audits remain the same—to verify the integrity of transactional data and assess internal controls. However, the volume of data is increased enormously, the tools are automatized, and the data analysis is implemented on a real-time or nearly real-time basis with predetermined benchmarks (Brown, Wong, & Baldwin, 2007; Chan, Chiu, & Vasarhelyi, 2018; Kuhn & Sutton, 2010).

A continuous audit provides multiple benefits to an organization and such audits are gaining more prominence in the profession (Munoko, Brown-Liburd, & Vasarhelyi, 2020). More frequent use of data and timely analysis increases audit quality and the thoroughness of internal controls, reducing a company's compliance risk (Kuhn & Sutton, 2010). The automation of audit procedures makes the cost of verifying more transactions relatively small with less demand for human resources (Brown et al., 2007). Behavioral impacts may occur as managers' decisions may change once they know they are being monitored (i.e., the so-called "Big Brother" effect; Brown et al., 2007; Kogan et al., 2018). Continuous audits also provide greater visibility to businesses that generate higher transparency for directors, investors, and other stakeholders (Deloitte, 2010). Some authors even state that companies that introduce continuous auditing often achieve rapid returns on their investments (Coderre & Police, 2005). Broadly, continuous audits provide an opportunity for value creation by saving potentially misused funds, improving a company's reputation, and reducing legal costs as well as improving the efficiency and effectiveness of the audit and compliance functions (Li, Dai, Gershberg, & Vasarhelyi, 2018).

To make these theoretical advantages feasible, frameworks for continuous audit have been developed to provide a more specific explanation of the approach.

Some authors have developed frameworks based on traditional audits (Du & Roohani, 2007). In these frameworks, a cycle starts when the auditor connects to the accounting information system and ends when the auditor disconnects (Chan & Vasarhelyi, 2011). Such frequent audit schemes address the need to reduce the time gap in the detection of fraud, but they still utilize manual techniques and rely on the materiality principle for data selection.

Other authors have described continuous audits as completely automatic analyses of all available data (Chan & Vasarhelyi, 2011). In this case, the auditor and the database have an ongoing connection with the help of IT applications. These applications trace the full data set according to predetermined rules and send alerts to the auditor when exceptions appear in the system. This continuous audit methodology leads to a shift in effort in the audit steps. Human resources are mainly needed for the planning or design steps, in which the rules for data analysis are determined, and to analyze exceptions.

2.2 | Data mining for an anticorruption audit

Modern companies create large amounts of information, or big data, and data systems are often integrated with the cloud, the Internet of Things, and external data sources, such as social media (Appelbaum, Kogan, & Vasarhelyi, 2017). Under these conditions, the audit department should have comprehensive tools to analyze big data for the purpose of identifying potential misstatements or risks of material misstatements as a result of corrupt or fraudulent actions.

Data mining is accepted as the most comprehensive tool for big data analysis for auditing purposes in compliance (Amani & Fadlalla, 2017; Gray & Debreceny, 2014). Moreover, a great share of corporate leaders lists it among their Top 10 priorities (Amani & Fadlalla, 2017). Data mining identifies patterns, rules, or models based on one or more populations of data; uses them to predict future outcomes; and highlights exceptions when the actual data fall outside of the predicted ranges or patterns (Gray & Debreceny, 2014).

Among data mining techniques, process mining has the greatest potential to generate value for anticorruption. It lies in the middle of the spectrum between very simple substantive tests and more complex and predictive techniques, which means it is relatively easy to implement but, at the same time, maintains its predictive ability (Amani & Fadlalla, 2017; Appelbaum et al., 2017; Gepp, Linnenluecke, O'Neill, & Smith, 2018). Process mining tests find differences between actual and designed processes and provide audit-relevant information in a manageable way. Process mining adds value in two ways. First, a series of process-mining tests narrows the sample of exceptions down to the risky ones, which reduces the data to a manageable size (Jans, Alles, & Vasarhelyi, 2013). Even more importantly, process mining provides a picture of how the process was undertaken in practice and the social relationships between individuals; auditors receive not only data entered by employees but also metadata or data about data that are recorded automatically and independently from individuals (Jans et al., 2013).

2.3 | Challenges with adopting technologies for anticorruption

Despite the visible advantages of continuous audit and data mining, implementing continuous audit still faces significant difficulties, which explains its low level of use in practice (Vasarhelyi et al., 2012). These difficulties include:

- Significant resources to invest.
- The complexity of designing and maintaining IT systems.
- Analyzing heterogeneous data.
- The necessary competence mix.

First, continuous auditing requires significant information system resources to operate at an optimal level, which is associated with significant costs (Appelbaum et al., 2017; Jans et al., 2013; Kuhn & Sutton, 2010). Design and maintenance concerns also arise when implementing continuous auditing because the initial volume of false alerts about exceptions, or the so-called "alarm flood," may be overwhelming, resulting in a system overload and unproductive time spent investigating nonissues (Appelbaum et al., 2017; Bumgarner & Vasarhelyi, 2018; Jans et al., 2013; Kuhn & Sutton, 2010). Multiple sources for automatic data capture are also a challenge, as audit functions need to systematize and unify different types of data and classifications from various heterogeneous business functions (Bumgarner & Vasarhelyi, 2018). The analysis of the final results and the design of the analytical rules for audits require human resources with extensive knowledge of enterprise resource planning (ERP) programing languages, which is costly and challenging (Debreceny, Gray, Ng, Lee, & Yau, 2005; Kuhn & Sutton, 2010).

To overcome these difficulties with implementing continuous auditing and data mining, researchers call for analytic studies, field experiments, and case studies to attempt to understand actual implementations of continuous auditing and data mining systems (Appelbaum et al., 2017; Brown et al., 2007; Jans et al., 2013). Additionally, the interconnection between continuous auditing, data mining, and process mining is an important area of future research that may uncover the most efficient combination of these processes for data analysis (Gray & Debreceny, 2014; Jans et al., 2013).

Moving forward from the literature review, our study aims to answer the following question:

1. RQ: How can continuous auditing and data mining be enabled for anticorruption purposes, and what are the critical factors for enabling these processes?

3 | RESEARCH METHODOLOGY AND DATA COLLECTION

We adopt a qualitative approach to answer our research question. A single case study is chosen as our methodology because it provides an opportunity to investigate the issue of continuous audit for anticorruption in a practical context in which the company's experience is

critical (Bhattacherjee, 2012), and it makes the findings intelligible to the reader (Dyer & Wilkins, 1991). The single case study allows us to explore the practical aspects of continuous audit theory in depth and find ways to practically implement the theoretical model in the context of anticorruption (Yin, 2014). A case study can help to understand detailed characteristics of and behaviors related to technology adoption by organizations (Vasarhelyi et al., 2012).

To support the analysis, we implement a research protocol (Yin, 2014) to validate the results (Table 1).

The construct validity of the research is assured by iterative work with theoretical assumptions and practical findings. We develop a theoretical model of continuous audit by adapting Chan and Vasarhelyi's (2011) model to the topic of anticorruption. The model is then verified with practical cases, and the empirical findings are again confirmed by the theoretical literature on continuous auditing, anticorruption, and big data. With this approach, we simultaneously increase both propositional and experiential knowledge (Stake, 2000).

For the internal validity of the results, the company used for the case study must first be rated in a continuous audit sphere, with anticorruption as the most urgent topic for audit implementation. With these criteria in mind, the Italian manufacturing company AST was chosen as the unit for the case analysis. AST is an Italian steel company with about 2,400 employees and a turnover of 1.8 billion EUR; its parent company is Thyssenkrupp (see reference WM1, WM2 reported in Table 2). AST was damaged by corruption prior to 2015, when it lost more than €100 million (i.e., raw material overpayments, sanctions, and legal costs) and suffered intangible costs (i.e., reputational damage and some members of senior management were prosecuted and arrested). In 2016, AST launched a transformational program based on the implementation of an automated continuous audit of all company transactions with process mining techniques and artificial intelligence (see reference CM1 in Table 2). This continuous audit for anticorruption allowed AST to prevent corruption losses and, furthermore, become one of the major Italian companies to receive ISO 37001 certification and the only steelwork company with this certification in Europe (see reference CM10 in Table 2).

Concerning the external validity of this study, case studies are designed to provide analytical rather than statistical generalizations (Yin, 2014). To enhance the generalizability of the results, the case findings are externally validated by theoretical references.

TABLE 1 Validation of the results

Test	Strategy	Phase
Construct validity	Continuous audit framework	Design of the study Construction of the findings
Internal validity	The case presents characteristics that justify the internal validity of the results	Selection of the case
External validity	Validation with external references	Construction of the findings

The reliability of the data is ensured by the triangulation of data sources (Stake, 2000; Yin, 2014; Table 2). Data are drawn from interviews with AST directors, internal official documents, and open sources (e.g., annual reports and websites). Moreover, we use not only AST materials but also presentations and reports from the parent company (Thyssenkrupp) as well as from other interested parties on the topic of anticorruption (e.g., peers, universities, and authorities). Informal meeting field notes, conference materials, and the AST website are used to initially adapt the theoretical model to the AST case, and the internal documents and questionnaires are used to verify our assumptions and provide more detail for the theoretical model.

4 | CONTINUOUS AUDITING MODEL FOR ANTICORRUPTION

We extend Chan and Vasarhelyi's (2011) framework with process mining as the most relevant analytical tool for anticorruption compliance.

Chan and Vasarhelyi's (2011) framework is chosen for this study because it explains the continuous audit process from the design stage to the reporting stage in a standardized way, meaning that the model is universal to any subject of auditing. This model is developed on the basis of several decades of research on the topic of continuous audit (Jans & Hosseinpour, 2019). Vasarhelyi and Halper (1991) define continuous audits, a 2004 study provides the principles for continuous auditing (Vasarhelyi, Alles, & Kogan, 2004), and a 2011 study updates them (Chan & Vasarhelyi, 2011). Thus, this framework is supported by a detailed review of the development of continuous audits and provides the most comprehensive understanding of innovation and advances in auditing using technology and automation.

As a result, we create a continuous audit model for anticorruption using a data mining tool (Figure 1). The model representation is based on the Gantt chart, one of the most popular and useful management tools (Wilson, 2003). It links the continuous audit framework to project management, making the model easy to read and implement in practice.

The blocks in our modified model (Model) are constructed based on the knowledge discovery in databases (KDD) framework. The KDD framework describes the overall process of extracting useful knowledge from data. It includes not only the revealing of patterns (data mining) but also the choices of encoding schemes, preprocessing, sampling, and data reduction (Fayyad, Piatetsky-Shapiro, & Smyth, 1996).

The first step in the model is creating (selecting) a data set for continuous audit. An auditor analyzes business processes to find possibilities for automatization. All major processes of each business unit should be described and inserted into the ERP system if possible. For the remaining data, manual data assurance (i.e., nonstandardized data assurance) is implemented at the end of the audit cycle. The result of this first step is a standardized data set of business processes.

Next, during the preprocessing step, the model for data analysis should be developed, and benchmarks for variables should be set.

TABLE 2 Data sources

Details	Organization	Contents	Date	Reference
Informal meeting field notes				
Governance Director and Business Continuity Officer	AST	Presentation of the Company and overview of the Internal Control System Approach	5 February 2018	FN1
Governance Director and Business Continuity Officer	AST	Enterprise Risk Management and Business Planning in AST	14 May 2018	FN2
Conference material				
Associate Director	AST	Legality Days: translate the commitment into action	26 November 2019	CM1
CEO	Torino Nord Ovest	Impact of technology on manufacturing, infrastructure and communication	26 November 2019	CM2
CTO	Acea Reti		26 November 2019	CM3
Co-founder and COO	Instal.com		26 November 2019	CM4
International Anticorruption Activities Coordinator	Ministry of Foreign Affairs	Impact of technology on legality	26 November 2019	CM5
Criminal Law Professor	SantAnna School of Advanced Studies		26 November 2019	CM6
Deputy Director of the Anti-corruption Master	Tor Vergata University		26 November 2019	CM7
Governance Director	AST	The Anticorruption Model of AST: smart solutions and instruments for continuous monitoring	26 November 2019	CM8
Head of Internal Control System	AST	The AST model: concrete examples	26 November 2019	CM9
Quality assurance director	AST	AST- the only steel company in Europe to have anti-corruption certification ISO 37001	26 November 2019	CM10
Associate Director	AST	The Anticorruption Model of AST: smart solutions and instruments for continuous monitoring	26 November 2019	CM11
Semi-structured interviews				
Governance Director and Business Continuity Officer	AST		23 May 2019	IS1
Head of Internal Control System	AST		23 May 2019	IS2
Internal documents				
Annual report	Thyssenkrupp		2018–2019	ID1
Policy for the prevention of corruption	AST		2019	ID2
Website releases				
Official company website of Thyssenkrupp (www.thyssenkrupp.com)	Thyssenkrupp		2019	WM1
Official company website of AST (www.acciaiterni.it)	AST		2019	WM2
Questionnaire (Appendix A)				
Head of Internal Control System	AST		20 January 2020	QR1

Benchmarks and models are established by applying estimation, classification, association, or clustering techniques to historical audited data (Chan & Vasarhelyi, 2011). Unlike in Chan and Vasaherlyi's framework, however, we do not include the testing step between building the model and running continuous auditing, as the test can be seen as one cycle that goes from the first to the

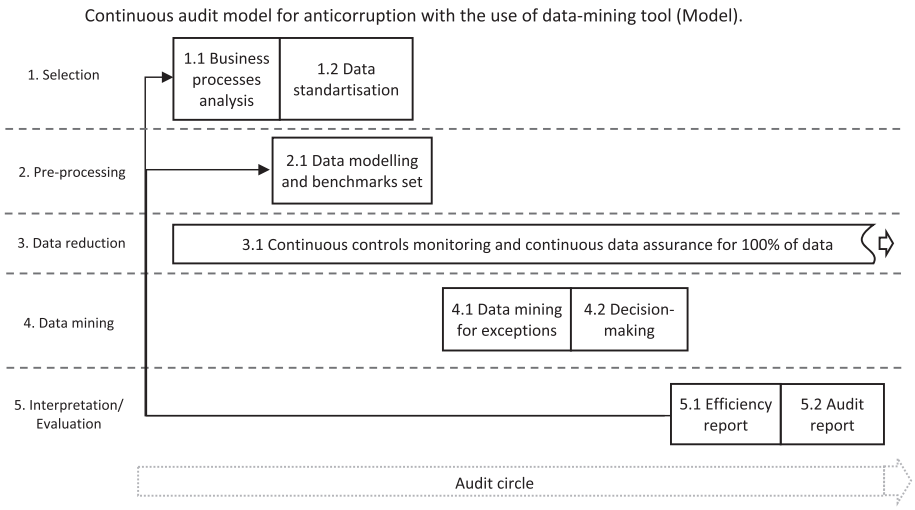

FIGURE 1 Continuous audit model for anticorruption with the use of data-mining tool (Model)

last step in the model over a shorter period of time compared with the usual one.

The third stage is undertaken continuously once it has started. It consists of two procedures aimed at reducing the data to a set of risky observations for further analysis. First, continuous control monitoring verifies whether employees undertook transactions in violation of internal control rules or anticorruption codes. Additionally, in continuous data assurance, transaction details are verified against benchmarks to identify outliers. Transactions involving internal control violations or anomalies (i.e., outliers) are red flagged as exceptions. In this stage, the program for continuous auditing in Chan and Vasaherlyi's model is supposed to be external. In the model, however, the programing tools can be either embedded or external (Kuhn & Sutton, 2010), depending on the company's ERP ecosystem. Moreover, Chan and Vasarhelyi's (2011) model suggests moving to direct reporting after a continuous audit if there are no outstanding material exceptions. However, the literature shows that this scenario is unrealistic. Moreover, the process may find too many exceptions, making manual analysis of the exceptions impossible (Appelbaum et al., 2017; Jans et al., 2013; Kuhn & Sutton, 2010). Thus, the next steps are devoted to automatic exception analysis.

In the fourth stage, data mining is implemented to detect the "exceptional exceptions." A great variety of data mining tools are available, and the step of choosing a tool may take a lot of time and effort. Thus, we propose concentrating on process mining, as it suits the anticorruption issue the most (Section 2). The process mining algorithm is used to search for data patterns. The technical data are translated into behavioral data to answer such questions as "Is the last employee who modified the transaction also the approver?" (Jans et al., 2013). The revealed metadata provide an understanding of the patterns of procedures for the selected business processes, and the appearance of some other patterns in minor groups is the reason for taking a closer look at those groups. Such minor groups or "exceptional exceptions" are analyzed using the walkthrough technique, in which the auditor follows a transaction from its origination through the company's processes (Jans et al., 2013). Outliers can be divided into four categories for further decision making: extreme values that are very logical when looked into, fraudulent actions, results of circumventing procedures, or mistakes. The first category is of no interest for audit, and fraudulent actions are supposed to be reported to management, whereas analyses of circumvented procedures and mistakes are used for fraud prevention (Jans, Lybaert, & Vanhoof, 2009).

In the fifth and final stages, reporting is undertaken. The auditor documents findings and resolutions and delivers them to management for further action regarding cases of corruption. Another report relates to the efficiency of the audit procedures themselves and includes such items as whether the continuous audit criteria revealed a manageable number of cases, whether some fraudulent cases may have been missed, the number of false alerts among the exceptions, and so on. The efficiency report is then used to adjust the model and benchmarks and to increase the automatization level of the processes and standardize the method of gathering data about the processes. Unlike in Chan and Vasarhelyi's model, the results of the reporting step are used in the next audit cycle, which creates a circulating system. This process allows the user to avoid keeping excessive data and to implement changes continually.

The model is created for one audit cycle (yearly/quarterly/daily). In the next cycles, the steps are repeated with modifications. The ongoing standardization of processes and efficiency checks can strengthen the accuracy of the audit. Continuous control monitoring is undertaken through all the cycles without interruption, and amendments to the working system are undertaken.

At the end of each audit cycle, knowledge is built as the end product of data-driven discovery (Fayyad et al., 1996). The derived knowledge adds value for compliance officers and CEOs by supporting decision making regarding suspicious transactions with understandable business process patterns for all data. Additionally, the audit results may be simply documented and reported to interested parties, providing the potential to increase trust between the company and its stakeholders.

5 | FINDINGS

Based on the model (Figure 1), we analyze AST's current model for anticorruption auditing by classifying AST's activities according to the theoretical steps. For these purposes, we suggest the practical realization of the model with the help of AST's materials and data, including conference material, internal documents, and website releases. We also sent a questionnaire based on Chan and Vasarhelyi's (2011) framework extended with process mining for anticorruption to AST's Head of Internal Control System (ICS; Appendix A). This questionnaire aims to clarify the company's experience, correct the specification of the model, and enrich it with practical examples for each step. The practical description of the model is also verified by scientific research papers. The results are presented in Table 3.

The continuous audit cycle for anticorruption at AST starts with process analyses, in which all business and support processes are analyzed for corruption risks and standardization possibilities. A full cycle of continuous audit is used for most risky and standardized processes, whereas others are processed with standard anticorruption tools (e.g., ombudsmen, hotlines, etc.) or with the limited usage of continuous audits (CM11). The processes that are most vulnerable to corruption are determined as follows: order to cash (payments), procure to pay (procurements), maintenance, investments, HR, and warehouse processes (QR1). Of these, the payments and procurements processes are inserted into ERP end-to-end, whereas the others are integrated partially (e.g., only the master data, timesheet entries, and payroll aspects of HR are inserted into ERP; QR1). Payments and procurements are the most standardized processes for any business and the most risky ones because of regular business relationships with third parties (Baader & Krcmar, 2018), which creates the motivation for continuous anticorruption auditing.

In the data standardization step, AST aggregates the data using an SAP system for all processes. Moreover, AST aggregates information from not only internal sources but also external sources, such as CRIBIS, AIDA, World Check, World Compliance, and Online Banking Statements (QR1, CM9, and CM11). Doing so allows for the verification of the internal data and incorporates relevant information for analysis. The data for analysis are uploaded in a dedicated separate

TABLE 3 AST case of the continuous auditing model for anticorruption

Element of the model		AST practice	References
1.	1.1 Business processes analysis	Most risky and most standardized processes are chosen	QR1, CM11
	1.2 Data standardization	Data sources for Payments: • SAP ERP (SAP FI, SAP MM), • Online Banking Statement. Data sources for Procurements: • SAP ERP (SAP FI, SAP MM, SP SD, SAP HR), • CRIBIS, AIDA, World Check, World Compliance.	QR1, CM9, CM11
2.	2.1 Data modeling and benchmarks set	Key indicators for Payments: • Payments out of working hours/days, • Frequent payments in a limited timeframe, • Payments made by unauthorized users, • Online Bank Statement vs Accounting Documents amount discrepancy. Key indicators for Procurements: • Frequent changes of Vendors Master Data, • Duplicated IBAN/VAT number, • PR/PO authorized just below the approval threshold, • Framework Agreements with unlimited Max Amount, • PO fragmentation, • Vendor/Quantity/Amount/Date/Material consistency along Purchasing process.	QR1, CM9, CM11
3.	3.1 Continuous controls monitoring and continuous data assurance for 100% of data	• Process Monitoring Cockpit (PMC), outside database storage, daily cycles, automatic daily alarms • Document verification	QR1, CM1, CM8, CM9
4.	4.1 Data mining for exceptions	1. Process mining 2. Deep dive with process owners	QR1, CM8, CM9
	4.2 Decision-making	Classification on fraud and risky transactions for further facilitation of fraud or process/system development	QR1, CM9
5.	5.1 Efficiency report	Business Intelligence feature of Process Monitoring Cockpit (PMC)	QR1, CM9, CM11, ID1
	5.2 Audit report	Reporting to ICS Department, Anti-Fraud Committee and Top Management	QR1, CM8, CM9

software module, called the Process Monitoring Cockpit (PMC), which guarantees independent control over IT activities and helps to avoid any slowdown in the working system (QR1). This modality is related to the monitoring control layer (MCL) audit tool, which operates independently of the information system to be monitored but is linked to it or its database (Kuhn & Sutton, 2010).

In the second step, data modeling and benchmark setting are carried out within a fraud risk assessment activity and through an IT feasibility analysis. Fraud risk assessment identifies applicable corruption schemes and monitors them, revealing the distinctive features of corrupt actions. These features are formalized in a list of benchmarks or indicators of corruption risk (CM9). In particular, AST has described 100 schemes with 40 benchmarks for all processes (CM9), including four indicators for payments and six indicators for procurement (Table 3, Part 2.1). The indicators of corruption risk that are identified during the fraud risk assessment are extrapolated to the relevant processes through the IT feasibility analysis, which verifies data availability and usability and builds an algorithm for data mining (QR1, CM9, and CM11).

The third step aims to reduce the full set of data to the potentially risky observations and is undertaken in two steps: continuous control monitoring and continuous data assurance.

Continuous control monitoring determines the transactions that have corruption risk according to predetermined benchmarks. For these purposes, the PMC monitors 5 million transactions per day in real time (QR1, CM1, and CM9). On a daily basis, the performance indicators return a list of approximately 2,000 flagged transactions that are analyzed by the ICS Department (CM9). Additionally, PMC users receive an e-mail when new occurrences appear on the dashboard (QR1, CM9). Continuous data assurance identifies actions that do not satisfy internal documentation rules (QR1). Manual document verification is undertaken to determine potentially anomalous transactions among the list of flagged transactions, reducing the data to approximately 10% of its original size. All of flagged transactions are investigated in detail by the ICS Department using IT systems or involving the process owners to distinguish real anomalies from false positives.

Data mining and process mining in particular are applied after the dataset has been reduced twice, which helps to avoid the main problem of continuous audit, that is, "alarm floods" (Appelbaum et al., 2017; Jans et al., 2013; Kuhn & Sutton, 2010). Process mining at AST is descriptive as opposed to predictive. It presents the metadata of transactions with suspicious transactions highlighted but without dividing them into simply fraudulent or legal categories. It allows circumvented procedures (explainable outliers) and mistakes to be tracked in data input, as these instances have the possibility to become opportunities for future fraud if they are not noticed initially (Jans et al., 2009). Even in such cases, the entire population of flagged transactions is checked by the ICS Department with IT systems and the process owners to detect real anomalies (QR1, CM8, and CM9).

Descriptive process mining requires manual decision-making over the final list of suspicious transactions (Jans et al., 2009). Anomalous transactions are accepted as fraudulent when the related controls regarding document verification, process mining, and the deep dive with process owners all fail (QR1 and CM9). Fraudulent occurrences are divided into two types according to a widely accepted classification (Jans et al., 2009). Actual fraud attempts lead to the summoning of the Anti-Fraud Committee and Crisis Committee, which is composed of top management (e.g., the CEO and the CFO) and whose main duties are to facilitate fraud investigations. Transactions that are not fraudulent (i.e., circumvented procedures and mistakes) indicate risky phenomena and require process or system improvements (QR1).

After decisions are made, they are inserted back into the system for system efficiency checks, in which the accuracy of alarms is analyzed. Every time a false positive is detected, that case is excluded from the subsequent run of the algorithm through a business intelligence feature of the PMC that allows the indicator settings to be automatically updated (QR1, CM9, and CM11). To avoid false negatives, fraudulent schemes are continuously updated through fraud risk assessment (ID1 and QR1).

The audit report with the revealed corruption cases is directed to the ICS Department and the Anti-Fraud Committee. Moreover, PMC alarms about anomalous occurrences may be directly reported to top management (i.e., the CEO and the CFO) if necessary (QR1, CM8, and CM9).

Overall, the model is integrated into the compliance system (WM1 and WM2). AST embeds it in three lines of the defense scheme (ID1 and ID2). The stages start with the "inform and advise" step, which involves the anticorruption education of personnel, and anticorruption regulations and guidance are transmitted to all companies. The "identify" step implies compliance audits, whistleblowing, ombudsmen, and risk analysis. The last step, called "report and act" includes reporting to the Board and the Audit Committee, corrective actions, and sanctions on fraud initiators (ID1 and ID2). These model stages are in line with the AST compliance system, which supports the validity of the theoretical model.

6 | DISCUSSION

To answer our research question, the AST experience shows the critical factors that are the pillars for implementing the model (Figure 1). These factors respond to the main challenges of implementing continuous auditing for anticorruption and are based on both AST's experience and the literature. The success factors describe the work within the continuous audit system and represent the changes needed in the organization to move from a traditional to a continuous audit and from manual to automated fraud detection (Table 4).

6.1 | Strategic vision and risk mapping

Anticorruption audits become efficient only by taking a strategic approach as opposed to a formal "check off" approach (Ashforth,

TABLE 4 Success factors of continuous audit for anticorruption at AST

Challenge (from literature)	AST success factor	References
Significant resources needed (Appelbaum et al., 2017; Jans et al., 2013; Kuhn & Sutton, 2010).	1. Strategic analysis and risk mapping	CM5, CM8, ID1, ID2, IS1, IS2, FN2
	2. No-corruption corporate culture	QR1, CM2, CM5, CM6, CM7, CM8, ID1, ID2, FN2, WM1, WM2
Human resources with extensive knowledge of programming and audit (Debreceny et al., 2005; Kuhn & Sutton, 2010)	3. Creating competence mix	QR1, CM1, CM4, CM8, CM9, CM11, ID1, IS1, IS2,
IT system design and maintenance (Appelbaum et al., 2017; Bumgarner & Vasarhelyi, 2018; Jans et al., 2013; Kuhn & Sutton, 2010)	4. IT infrastructure	QR1, CM3, CM9, CM11
Heterogeneous data to analyze (Appelbaum et al., 2017; Bumgarner & Vasarhelyi, 2018; Jans et al., 2013; Kuhn & Sutton, 2010)	5. Effective process design	CM2, CM8, CM9, CM11, FN1

Gioia, Robinson, & Treviño, 2008). Thus, corporate governance should be carried out to ensure ethics and responsibility (CM5). Positioning anticorruption within the corporate strategy helps not only in attracting more funding for an anticorruption audit but also in boosting operational synergies between business units and establishing company-wide anticorruption activities (Cardoni, Kiseleva, & Lombardi, 2020).

A continuous audit also requires a strategic level that allows intercompany synergies. Such synergies are of paramount importance because continuous audits highly overlap with the need for functional management (Alles, Kogan, & Vasarhelyi, 2008).

Thus, a company is expected to manage corruption with strategic risk management tools, assess the likelihood and impact of corruption in each sphere, and establish appropriate internal control measures for each sphere (Jeppesen, 2019). Continuous auditing should first be established for the riskiest processes to reduce resource demand.

At AST, the integration and establishment of measures related to anticorruption is the focus of the compliance strategy, which is defined by the Board (FN2 and ID1). The ICS Director, who is directly accountable to the Anti-Fraud Committee and the Board of Directors, is responsible for anticorruption and the anticorruption audit (ID2, IS1, and IS2). The high positioning of the anticorruption issue enables its corporate-wide implementation and allows for synergies between all the stakeholders of the continuous audit (CM8). The internal control system at AST is integrated with corporate risk management, which is built as a model with three lines of defense (Section 5) and is aligned to the Committee of Sponsoring Organizations of the Treadway Commission's Enterprise Risk Management framework (ID1; Committee of Sponsoring Organizations of the Treadway Commission, 2017a; Committee of Sponsoring Organizations of the Treadway Commission, 2017b). With the help of risk management, the two most risky processes, procurements and payments, are analyzed with continuous audit, reducing system overload (CM11).

6.2 | No-corruption corporate culture

Regardless of the strength of the anticorruption audit, management can still override internal controls, creating a vicious cycle in which more sophisticated controls lead to more advanced corruption schemes (Appelbaum et al., 2017). Continuous auditing, as an enabling technology, must enable not only technical changes but also profound cultural change, which is more important (CM2 and CM5). Fraud prevention should take precedence over detection when a company creates a work environment that values honesty (Davia, 2000; Jans et al., 2009). Minimizing opportunities for fraud is of paramount importance and is supposed to be the only element of fraud risk that employers can influence (Jans et al., 2013; Wells, 2003).

The vision of the fight against corruption is holistic, and the multistakeholder approach is central. In other words, businesses, civil society, and researchers are called to share control over legal issues (CM5 and CM6). The community should be the primary interest of the company (CM7).

Thus, AST implements a mindset approach to anticorruption, creating a unified culture of zero tolerance to corruption. AST also uses the "lead by example" principle, which means that it must serve as an example for other businesses and society in the fight against anticorruption. The third principle, "equilibrium," implies that there is no trade-off between performance and control, results and rules, or business and values (ID1, ID2, WM1, and WM2). These anticorruption principles are fixed in AST's normative documents (e.g., the Code of Conduct and the Supplier Code of Conduct) and are translated throughout all companies by means of educational seminars, e-learning courses, and conferences (FN2, CM8, and WM1).

6.3 | Creating competence mix

Auditor education and familiarity with analytics is a limiting factor in implementing continuous audits (Appelbaum et al., 2017; Ranjan,

Jha, & Pal, 2016). An auditor must manage comprehensive situations and be able to navigate multitasking teams built from audit departments, compliance officers, risk managers, IT specialists, and representatives of different functions (CM1, CM8, CM9, and CM11). Continuous audits are connected to IT technologies to a large degree, and, thus, auditors must have expertise in general IT controls, such as data access, integrity, change protocols, and security (KPMG, 2018). Because universities are not yet able to provide such qualifications (IS1, IS2, and CM4), companies may organize training that covers general audit knowledge (e.g., internal control, audit methodology, etc.) as well as specific IT knowledge, such as tools for data analysis, work flow, and working paper instruments (Vasarhelyi et al., 2012).

According to AST's ICS Director, "The machine is designed by man, it serves to support man, but does not replace it" (CM9). The mix of competencies in both compliance and risk management fields and the knowledge of massive analysis activities, scientific approaches, psychology, and typical business skills have brought great added value to AST (QR1, CM8, and CM9).

To provide employees with multiple skills, AST undertakes classroom courses and e-learning on antitrust law and corruption prevention (ID1). ICS departments organize events for knowledge cross fertilization between specialists (e.g., the conference called "Artificial Intelligence: New Technologies, Legality and Fight against Corruption" held on November 26, 2019; CM9 and CM11). A silo mentality, in which some departments or groups within an organization do not want to share information or knowledge with others, is not acceptable (CM8). Apart from educational programs and events, the company is designing a motivational scheme for employees to learn about anticorruption activities by including anticorruption key performance indicators in performance evaluation schemes for both compliance officers and function managers (IS1 and IS2).

6.4 | Effective process design

IT infrastructure helps to accumulate diverse data, but it does not solve the data heterogeneity problem, which is expected to be one of the main limiting factors for continuous audit implementation (Fayyad, Piatetsky-Shapiro, & Smyth, 1996; Rezaee, Sharbatoghlie, Elam, & McMickle, 2002). The fundamental feature of continuous audit technology is a change in the audited processes (CM2). A company not only must insert processes into ERP and use continuous audit applications but must also model and redesign its business processes according to its global system. Business design therefore needs to be shifted from a fragmented, functional-based structure to a process-based integrated system (Al-Mashari, 2003).

For data standardization, AST undertakes two measures. The IT department unifies the language across the programming for all processes by mapping data to a single naming convention, uniformly representing and handling missing data and handling noise and errors when possible (CM8, CM9, and CM11). At the same time, the ICS Department builds a common language for the company; it redesigns business procedures together with the process owners (functional managers) to ensure that the SAP and continuous audit modules can be accommodated within the entire business operation (FN1).

6.5 | IT infrastructure

The issue of anticorruption is cross-functional (Cardoni et al., 2020). Thus, auditors must accumulate big data from different business units, which usually have specific business processes011, legacy system control settings, transaction processes, IT processes, and so forth. (Kuhn & Sutton, 2010; Vasarhelyi et al., 2012). ERP allows the aggregation of the data on all processes of all organizations in the database, and such applications as the MCL or embedded audit modules can also be used, particularly for continuous auditing of the data. MCL may be the optimal option for big and diverse businesses, as it is controlled outside of the company's ERP and does not require the creation of difficult embedded code for all types of data (Kuhn & Sutton, 2010).

AST uses SAP as its ERP software and the PMC as an outside continuous audit provider to simplify the process of aggregating data from different departments (QR1). As a result, 10 processes, or 5 million transactions per day, are available for continuous analysis (CM9 and CM11). At the same time, the data processing effort is much more focused, allowing for a higher level of analysis and prediction (CM3).

6.6 | Critical elements of the model

The continuous audit model for anticorruption has brought fruitful results to AST in terms of reduced corruption losses, increased reputation, and ISO 37001 certification (CM10). The internal audit function appears to be not only a control mechanism but also a cultural element of the company. It has become more strategy-oriented, digitalized, and more imbedded into other functions and business units.

Nevertheless, the AST model is not completely mature. According to Vasarhelyi et al. (2012), the AST continuous audit model for anticorruption may be classified as being somewhere between emerging and mature continuous audits. AST has almost all characteristics of the mature model, including continuous control monitoring, alarms and follow-up processes, an automated monitoring module, integration with risk management, natural process synergies, monitoring at the transactional level, and other characteristics. However, its model still has space to grow.

The main direction of continuous audit development is increasing the proportion of all processes covered by the model. AST implements continuous audit for its riskiest functions, whereas others are checked using traditional auditing tools (QR1). The coverage of the model may be increased through the ongoing standardization of processes across functions, their integration into the ERP system, and the development of anticorruption benchmarks for new functions. A mature continuous audit process monitors the internal controls and operations of each branch continuously (Vasarhelyi et al., 2012). Greater system coverage can bring a critical meta-control structure, deep cooperation, and cross-fertilization between the control, audit, and risk functions and

other business units and common effective infrastructures (Vasarhelyi et al., 2012).

Apart from this coverage issue, the data extraction method matters. AST has daily data accumulation cycles, which are very close to ongoing real-time monitoring. However, this features still corresponds to emerging continuous audit practices, in which key extractions are repeated on a cyclical basis (Vasarhelyi et al., 2012). The implementation of a technical solution for real-time monitoring systems can bring new opportunities for system development in terms of automatization levels.

7 | CONCLUSIONS

In the modern digital world, continuous audit is becoming an innovative technique and a necessity for any business. The ongoing, timely review of all data is relevant for today's challenges, including big data, new technologies, globalization, tight law enforcement, and so forth.

Anticorruption requires continuous audit because of its detrimental impact on a company's financial performance and reputation. Moreover, corruption risk is a peculiar type of risk that cannot be reduced or accepted but must be eliminated or avoided at its core. For this aim, continuous audit is the only acceptable method for anticorruption checks, as it tracks all business transactions on an everyday basis. Despite this fact, the connection between continuous audits and corruption has not been studied thoroughly.

Our study fills this gap in research on continuous auditing by examining the expansion of the continuous audit model to the anticorruption issue. We adapted one of the most comprehensive continuous audit frameworks, that of Chan and Vasarhelyi (2011), to this particular issue and expanded it to include the features of an anticorruption audit. In particular, the modified model is cyclical with efficiency reports and the ability to immediately insert changes into an ongoing continuous monitoring process, which introduces a dynamic self-learning mechanism. Exceptions analysis is automated, which reduces the issue of "alarm floods." The usage of process mining in the framework narrows down the vast variety of technical tools to the most appropriate ones for anticorruption audits.

This study may be used in practice by compliance officers, internal auditors, and CEOs in planning continuous audit implementation as part of compliance. The proposed model includes particular practical steps according to the KDD framework, which makes the model closer to an IT framework. Moreover, the steps are represented with a well-known managerial tool, the Gantt chart, which allows it to be used directly in planning.

Success factors are also of paramount importance for practitioners, as they describe the key organizational issues that must be solved to efficiently implement the model. They show that effective continuous audits are centered on an integrative approach and elements of change management (Al-Mashari, 2003). With the help of the AST case, we have revealed that these elements include a strategic vision and risk mapping as well as a no-corruption corporate culture. They enable the model to be implemented by a company and prepare employees for compliant behavior, preventing corruption at its core. Moreover, people, processes, and technology are the three drivers of change management for any ERP project (Ranjan et al., 2016). Educated employees with competencies in IT, data analysis, compliance, business operations, and even psychology enable harmonized and efficient work at each step of the model. Correct process redesign allows processes to be homogenized across the company for easy insertion into the IT system. At the same time, the IT infrastructure provides a technical basis for process standardization and integration for continuous audit applications.

As a single case study (Yin, 2014), the model expands and generalizes the theory of continuous audit for anticorruption issues. The theoretical generalizability is supported by the vast literature on continuous auditing, anticorruption management, data mining, and process mining.

From a practical perspective, the model can be adapted for manufacturing businesses or any other sector, as is described in the example of standard processes (e.g., procurements and payments) used by almost all businesses (Baader & Krcmar, 2018). The model can be implemented by companies that have an ERP system, which is used as a basic element for data accumulation in continuous audits. ERP systems may incur significant costs; thus, we suggest that the model is primarily suitable for large enterprises. Additionally, a crucial requirement is related to the very high level of managerial knowledge required to design and implement the model. In the case of AST, the innovation in the model was developed by skilled senior staff, most of whom had previous experience in consulting and auditing firms and the right attitudes and competencies to integrate strategy, risk management, organizational processes, and compliance. Owing to the effective design and the holistic approach adopted, technology and managerial culture represent the pillars of the model and have inspired the right solutions to manage the relationship between the bureaucratization of work and the efficiency of organizational processes.

There are several directions for future research. Although the single case study method is advantageous because it allows for deep analysis, it is also a limiting factor of this study. Further analysis may focus on cases in other countries or sectors of the economy with high corruption risk. Additionally, this study is based on the assumption that a company uses an ERP system, but it is predicted that cloud systems may be more prevalent in the future (Kogan et al., 2018). The adaptation of this issue to cloud computing may be of particular interest. Finally, this study does not discuss the role of managers in the new auditing model. The impact of new technology on the compliance decision-making process and whether it can be automated are also open questions for future research.

ACKNOWLEDGEMENTS

One of the authors (E.K.) is attending the program I.Ph.D.@UNIPG.

ORCID

Andrea Cardoni https://orcid.org/0000-0002-2216-1601
Francesco De Luca https://orcid.org/0000-0002-3501-9356

REFERENCES

Alles, M. G., Kogan, A., & Vasarhelyi, M. A. (2008). Putting continuous auditing theory into practice: Lessons from two pilot implementations. *Journal of Information Systems*, *22*(2), 195–214. https://doi.org/10.2308/jis.2008.22.2.195

Al-Mashari, M. (2003). A process change-oriented model for ERP application. *International Journal of Human–Computer Interaction*, *16*(1), 39–55. https://doi.org/10.1207/S15327590IJHC1601_4

Amani, F. A., & Fadlalla, A. M. (2017). Data mining applications in accounting: A review of the literature and organizing framework. *International Journal of Accounting Information Systems*, *24*, 32–58. https://doi.org/10.1016/j.accinf.2016.12.004

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory*, *36*(4), 1–27. https://doi.org/10.2308/ajpt-51684

Ashforth, B. E., Gioia, D. A., Robinson, S. L., & Treviño, L. K. (2008). Reviewing organizational corruption. *Academy of Management Review*, *33*(3), 670–684. https://doi.org/10.5465/amr.2008.32465714

Association of Certified Fraud Examiners. (2018). Report to the nations. *2018 Global Study on Occupational Fraud and Abuse*. Retrieved from https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf

Baader, G., & Krcmar, H. (2018). Reducing false positives in fraud detection: Combining the red flag approach with process mining. *International Journal of Accounting Information Systems*, *31*, 1–16. https://doi.org/10.1016/j.accinf.2018.03.004

Bhattacherjee, A. (2012). Case Research. *Social science research principles, methods and practices*, Textbooks Collection3, 2(93–103). Tampa, Florida, USA: University of South Florida. http://scholarcommons.usf.edu/oa_textbooks/3

Brown, C. E., Wong, J. A., & 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. https://doi.org/10.2308/jeta.2007.4.1.1

Bumgarner, N., & Vasarhelyi, M. A. (2018). Continuous auditing—A new view. In Y. C. David, C. Victoria, & A. V. Miklos (Eds.), *Continuous auditing* (pp. 7–51). https://doi.org/10.1108/978-1-78743-413-420181002

Cardoni, A., Kiseleva, E., & Lombardi, R. (2020). A sustainable governance model to prevent corporate corruption: Integrating anticorruption practices, corporate strategy and business processes. *Business Strategy and the Environment*, *29*(3), 1173–1185. https://doi.org/10.1002/bse.2424

Chan, D. Y., Chiu, V., & Vasarhelyi, M. A. (2018). Continuous Auditing—A New View. *Continuous auditing: Theory and application*, (7–51). Bingley, United Kingdom: Emerald Group Publishing. https://doi.org/10.1108/9781787434134

Chan, D. Y., & Vasarhelyi, M. A. (2011). Innovation and practice of continuous auditing. *International Journal of Accounting Information Systems*, *12*(2), 152–160. https://doi.org/10.1016/j.accinf.2011.01.001

Chiu, V., Liu, Q., & Vasarhelyi, M. A. (2014). The development and intellectual structure of continuous auditing research. *Journal of Accounting Literature*, *33*(1), 37–57. https://doi.org/10.1016/j.acclit.2014.08.001

Cipriano, H. M., Pereira, R., Almeida, R., & da Silva, M. M. (2019). Addressing continuous auditing challenges in the digital age: A literature review. In *Organizational auditing and assurance in the digital age* (pp. 153–171). https://doi.org/10.4018/978-1-5225-7356-2.ch008

Coderre, D., & Police, R. C. M. (2005). *Global technology audit guide: Continuous auditing implications for assurance, monitoring, and risk assessment* (pp. 1–34). Lake Mary, Florida, USA: The Institute of Internal Auditors.

Committee of Sponsoring Organizations of the Treadway Commission. (2017a). Enterprise risk management. Integrating with strategy and performance. Retrieved from https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Committee of Sponsoring Organizations of the Treadway Commission. (2017b). Fraud risk management guide. Retrieved from https://www.coso.org/documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf

Davia, H. R. (2000). *Accountant's guide to fraud detection and control* (2nd ed.). Retrieved from https://trove.nla.gov.au/version/45655460

Debreceny, R. S., Gray, G. L., Ng, J. J., Lee, K. S., & Yau, W. (2005). Embedded audit modules in enterprise resource planning systems: Implementation and functionality. *Journal of Information Systems*, *19*(2), 7–27. https://doi.org/10.2308/jis.2005.19.2.7

Deloitte. (2010). Continuous monitoring and continuous auditing. From idea to implementation.

Du, H., & Roohani, S. (2007). Meeting challenges and expectations of continuous auditing in the context of independent audits of financial statements. *International Journal of Auditing*, *11*(2), 133–146. https://doi.org/10.1111/j.1099-1123.2007.00359.x

Dyer, W. G., & Wilkins, A. L. (1991). Better stories, not better constructs, to generate better theory: A rejoinder to eisenhardt. *The Academy of Management Review*, *16*(3), 613–619. https://doi.org/10.2307/258920

Fayyad, U., Piatetsky-Shapiro, G., Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI magazine*, *17*(3), 37–37

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). The KDD process for extracting useful knowledge from volumes of data. *Communications of the ACM*, *39*(11), 27–34. https://doi.org/10.1145/240455.240464

Gepp, A., Linnenluecke, M. K., O'Neill, T. J., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. *Journal of Accounting Literature*, *40*, 102–115. https://doi.org/10.1016/j.acclit.2017.05.003

Gray, G. L., & Debreceny, R. S. (2014). A taxonomy to guide research on the application of data mining to fraud detection in financial statement audits. *International Journal of Accounting Information Systems*, *15*(4), 357–380. https://doi.org/10.1016/j.accinf.2014.05.006

Groomer, S. M., & Murthy, U. S. (2018). Continuous Auditing of Database Applications: AnEmbedded Audit Module Approach. In D. Y. Chan, V. Chiu, & M. A. Vasarhelyi (Eds.), *Continuous Auditing* (pp. 105–124). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78743-413-420181005

Jans, M., Alles, M., & Vasarhelyi, M. (2013). The case for process mining in auditing: Sources of value added and areas of application. *International Journal of Accounting Information Systems*, *14*(1), 1–20. https://doi.org/10.1016/j.accinf.2012.06.015

Jans, M., & Hosseinpour, M. (2019). How active learning and process mining can act as continuous auditing catalyst. *International Journal of Accounting Information Systems*, *32*, 44–58. https://doi.org/10.1016/j.accinf.2018.11.002

Jans, M., Lybaert, N., & Vanhoof, K. (2009). A framework for internal fraud risk reduction at IT integrating business processes: The IFR^2 framework. *The International Journal of Digital Accounting Research*, *9*(15), 1–29. https://doi.org/10.4192/1577-8517-v9_1

Jeppesen, K. K. (2019). The role of auditing in the fight against corruption. *The British Accounting Review*, *51*(5), 100798–100824. https://doi.org/10.1016/j.bar.2018.06.001

Kogan, A., Sudit, E. F., & Vasarhelyi, M. A. (2018). Continuous online auditing: A program of research. In D. Y. Chan, V. Chiu, & M. A. Vasarhelyi (Eds.), *Continuous Auditing* (pp. 125–148). https://doi.org/10.1108/978-1-78743-413-420181006

KPMG. (2018). 20 key risks to consider by internal audit before 2020. Retrieved from https://assets.kpmg/content/dam/kpmg/ch/pdf/key-risks-internal-audit-2018.pdf

Kuhn, J. R., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The current state and future directions. *Journal of*

Information Systems, *24*(1), 91–112. https://doi.org/10.2308/jis.2010.24.1.91

Li, H., Dai, J., Gershberg, T., & 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. https://doi.org/10.1016/j.accinf.2017.12.005

Lombardi, R., Trequattrini, R., Cuozzo, B., & Cano-Rubio, M. (2019). Corporate corruption prevention, sustainable governance and legislation: First exploratory evidence from the Italian scenario. *Journal of Cleaner Production*, *217*, 666–675. https://doi.org/10.1016/j.jclepro.2019.01.214

Munoko, I., Brown-Liburd, H. L., & Vasarhelyi, M. (2020). The ethical implications of using artificial intelligence in auditing. *Journal of Business Ethics*., 1–26. https://doi.org/10.1007/s10551-019-04407-1

Ranjan, S., Jha, V. K., & Pal, P. (2016). Literature review on ERP implementation challenges. *International Journal of Business Information Systems*, *21*(3), 388–402. https://doi.org/10.1504/IJBIS.2016.074766

Rezaee, Z., Sharbatoghlie, A., Elam, R., & McMickle, P. L. (2002). Continuous auditing: Building automated auditing capability. *Auditing: A Journal of Practice & Theory*, *21*(1), 147–163. https://doi.org/10.2308/aud.2002.21.1.147

Stake, R. E. (2000). Case studies. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (pp. 435–453). Thousand Oaks, CA: SAGE.

The Greens/EFA in the EU Parliament. (2018). The cost of corruption across the EU. Retrieved from https://www.greens-efa.eu/files/doc/docs/e46449daadbfebc325a0b408bbf5ab1d.pdf

UN Global Compact. (2019). The sustainable development goals report 2018. Retrieved from https://unstats.un.org/sdgs/files/report/2018/TheSustainableDevelopmentGoalsReport2018-EN.pdf

Vasarhelyi, M. A., Alles, M., Kuenkaikaew, S., & 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. https://doi.org/10.1016/j.accinf.2012.06.011

Vasarhelyi, M. A., Alles, M., & Williams, K. T. (2010). The Now Economy. *Continuous assurance for the now economy*, (9–33). Sydney, Australia: Institute of Chartered Accountants. http://raw.rutgers.edu/docs/Continuous%20Audit%20library/australia_mav__march%203.pdf

Vasarhelyi, M. A., Alles, M. G., & Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. *Journal of Emerging Technologies in Accounting*, *1*(1), 1–21. https://doi.org/10.2308/jeta.2004.1.1.1

Vasarhelyi, M. A., & Halper, F. B. (1991). The continuous audit of online systems. V. Chiu & M. A. Vasarhelyi *Auditing: A Journal of Practice and Theory*, Rutgers Studies in Accounting Analytics, 110–125). Bingley, United Kingdom: Emerald Publishing Limited.

Wells, J. T. (2003). Corruption: Causes and cures. *Journal of Accountancy*. Retrieved from https://www.journalofaccountancy.com/issues/2003/apr/corruptioncausesandcures.html

Wilson, J. M. (2003). Gantt charts: A centenary appreciation. *European Journal of Operational Research*, *149*(2), 430–437. https://doi.org/10.1016/S0377-2217(02)00769-5

Yin, R. K. (2014). Designing Case Studies. *Case study research: Design and methods (Sage publications)*, 5(18–54). Thousand Oaks, CA, USA: Sage.

How to cite this article: Cardoni A, Kiseleva E, De Luca F. Continuous auditing and data mining for strategic risk control and anticorruption: Creating "fair" value in the digital age. *Bus Strat Env*. 2020;29:3072–3085. https://doi.org/10.1002/bse.2558

APPENDIX A: The questionnaire for Model verification

General questions:

1 Which business functions are analyzed for anticorruption (customer relations, supplier relations, other)?
   1.1 What share of the processes of these functions are inserted into ERP (or other internal database)?
1 What were the main difficulties in implementing 100% data analysis?
2 Which factors helped in successful implementation of 100% data analysis (employee training at audit department/standardization of processes/other)?

Questions based on Chan and Vasarhelyi (2011) framework as extended with process mining for anticorruption:

Step	Questions	Answers for payments process	Answers for supplier assessment process
Selection	1.1 Which internal data sources are used for analysis (ERP/other)?		
	1.2 Which external data sources are used for analysis?		
Pre-processing	2.1 Which key indicators are used for audit?		
	2.2 How are these key indicators chosen for analysis?		
Data reduction	3.1 Which IT programs/systems are used for continuous analysis of 100% of data? Is it an online system?		
	3.2 How is the security of the data assured (outsourcing of IT system/ghost system/other)?		
	3.3 How often is the audit of 100% of data undertaken?		
	3.4 Does the system have automatic alarms about potentially anomalous occurrences?		
Data-mining	4.1 What does the analyses of potentially anomalous occurrences include (transaction tests, ratio analysis, sampling, clustering, process mining, Bayesian theory, probability theory models, regressions, other)?		
	5.1 How often is the analyses of potentially anomalous occurrences?		
	6.1 What are the rules for accepting anomalous occurrences as fraudulent?		
Interpretation/Evaluation	7.1 How is the amount of false alarms controlled?		
	7.2 How are new fraudulent schemes discovered?		
	8.1 Who are the users of reporting on anticorruption audit?		