A Field Study on the Use of Process Mining of Event Logs as an Analytical Procedure in Auditing

Mieke Jans
Hasselt University

Michael G. Alles
Miklos A. Vasarhelyi
Rutgers, The State University of New Jersey, Newark

ABSTRACT: There is a large body of accounting research literature examining the use of analytical procedures by auditors and proposing either new types of analytical procedures or more effective ways of implementing existing procedures. In this paper, we demonstrate—using procurement data from a leading global bank—the value added in an audit setting of a new type of analytical procedure: process mining of event logs. In particular, using process mining, we are able to identify numerous transactions that we consider to be audit-relevant information, including payments made without approval, violations of segregation of duty controls, and violations of company-specific internal procedures. Furthermore, these identified anomalies were not detected by the bank's internal auditors when they conducted their examination of that same data using conventional audit procedures, thus establishing the benefits of using process mining to complement existing audit methods. Process mining is a very different approach to evidence collection and analysis as it does not focus on the value of transactions and its aggregations, but on the transactional processes themselves. In addition to demonstrating the benefits of process mining in an audit context, this paper also discusses the contributions that process mining can make both to accounting research and auditing practice.

Keywords: process mining; analytical procedures; auditing; event logs.

I. INTRODUCTION

S tatement of Auditing Standard AU Section 329 (PCAOB 2010) specifies that analytical procedures are an integral part of the audit process in testing for relationships that exist between transactions.[1] External and internal auditors use analytical procedures to search for significant differences between observed data and expectations models. This enables the detection of anomalous transactions that may indicate financial accounting irregularities, breakdowns in internal controls, and/or fraud. A large body of accounting research examines the use of analytical procedures by auditors and proposes either new types of analytical procedures or more effective ways of implementing existing procedures (Hylas and Ashton 1982; Kinney 1987; Loebbecke and Steinbart 1987; Biggs, Mock, and Watkins 1988; Knechel 1988; Wright and Ashton 1989; Hirst and Koonce 1996; Wilks 2002; O'Donnell and Schultz 2003, 2005; Carpenter 2007; Peecher, Piercey, Rich, and Tubbs 2010; Brewster 2011).

Process mining of event logs is a method for understanding how complex business processes operate. It has been developed over the last decade by computer scientists and statisticians in collaboration with such leading corporations as SAP and Phillips. Jans, Alles, and Vasarhelyi (2013) state: "The basic idea of process mining is to extract knowledge from event logs recorded by an information system" where an *event log* is "a chronological record of computer system activities which are saved to a file on the system." Process mining is thus the systematic analysis of the data automatically recorded by a modern information technology system, such as the Enterprise Resource Planning systems (ERP) that form the IT infrastructure of most large- and medium-sized businesses today.[2]

Process mining allows businesses to undertake a fact-based identification of problems in their business processes (van der Aalst 2011) to facilitate comparison of the actual processes against the designed processes. Despite extensive use in such areas as business process improvement, healthcare, and network security, process mining has yet to be implemented in auditing, although van der Aalst, van Hee, van Werf, and Verdonk (2010) and Jans et al. (2013) make the conceptual case that it might add value.[3] Whether process mining would add value when applied to auditing is an empirical question that can be evaluated by using the method in an actual audit setting. This paper extends the preliminary work of Jans, Depaire, and Vanhoof (2011) that focused on applying process mining algorithms to event logs obtained from a European bank. In the business process modeling research literature the application of new algorithms is by itself of added value. The focus of this paper, which re-analyzes those event logs, is not on process mining as an end in itself, but as a means toward the end of adding value as an analytical procedure in auditing. This paper also

---

[1] "Analytical procedures are an important part of the audit process and consist of evaluations of financial information made by *a study of plausible relationships among both financial and nonfinancial data*. Analytical procedures range from simple comparisons to the use of complex models involving many relationships and elements of data. *A basic premise underlying the application of analytical procedures is that plausible relationships among data may reasonably be expected to exist and continue in the absence of known conditions to the contrary*. Particular conditions that can cause variations in these relationships include, for example, specific unusual transactions or events, accounting changes, business changes, random fluctuations, or misstatements" (PCAOB 2010, emphasis added).

[2] The market leading and best known ERP vendor is the German firm SAP™.

[3] The idea of mining the process in a context of workflow processes was introduced by Agrawal, Gunopulos, and Leymann (1998). Over the last decade, research in this domain has expanded greatly as many different aspects of business process mining have been developed and investigated by researchers from a variety of disciplines (Bozkaya, Gabriels, and van der Werf 2009; de Medeiros, Weijters, and Aalst 2006; Folino, Greco, Guzzo, and Pontieri 2009; Greco, Guzzo, Pontieri, and Saccà 2006; Gunther and van der Aalst 2007; Rozinat and van der Aalst 2008; van der Aalst, Schonenberg, and Song 2011; van der Aalst et al. 2003; van Dongen, de Medeiros, Verbeek, Weijters, and van der Aalst 2005; van der Aalst et al. 2010; Jans, Lybaert, and Vanhoof, 2010; Jans 2009). Jans et al. (2013) provide a literature review on the process mining literature.

utilizes different algorithms from Jans et al. (2011), as well as developing metrics oriented to audit practice and providing a linkage to the extant audit research literature.

The data analyzed by process mining consists of the event log that the auditor constructs from records maintained by a business's information systems. What is particularly promising about using the event log as a basis for analytical procedures is that it consists not only of data entered by the auditee, but also meta-data (data about data) that is recorded automatically and independently of the persons and processes whose behavior is the subject of the audit (Jans et al. 2013). This contrasts with current analytical procedures, which rely mainly on data entered by the auditee. Moreover, the potential of process mining extends beyond standard data analysis to provide new forms of analytical procedure tests that may yield insights that exceed those obtainable from commonly used audit tools.

Process mining is distinctive as an audit tool because it focuses on the path of transactions and not directly on the validation of the values in the associated process. It is thus a powerful tool for tests of controls, such as those for segregation of duties. Process mining is also applied to the population of data rather than to a sample as in traditional auditing procedures. Process mining is thus both a product of the computerization of business and a means of exploiting that new reality.

This study demonstrates the value of process mining by applying it to actual data from one of Europe's largest banks. Process mining of this data identifies audit-relevant information not previously detected by the bank's internal auditors when they examined that same data. This observation supports the argument that process mining gives auditors new information not obtainable otherwise from current audit procedures.

Process mining of event logs identified numerous anomalous transactions, including those concerning payments made without approval, violations of segregation of duty controls, and violations of company-specific internal procedures. These anomalies were not detected by the internal auditors when they conducted their own examination using conventional manual and IT-based audit procedures. Although this study does not determine whether the identified irregularities are indications of fraud, failed controls, or legitimate transactions, it establishes that process mining identifies potentially problematic issues not detected by existing audit techniques. While the generality of these conclusions is constrained by the specificity of the context, the results do suggest the potential of process mining as a promising new analytical procedure in auditing. The results of this field study also indicate the need for further work by academic researchers and practitioners in order to better delineate the specific circumstances in which process mining can add value.

This study also contributes to the literature by expanding the domain of audit research from primarily focusing on transactional data entered by the auditee to the meta-data on the business process that gave rise to that transaction. Over the last few years, accounting researchers have used text-mining tools to extend the domain of their research from quantitative financial data to qualitative information contained in annual reports, transcripts of analysts' calls, and the like (Li 2010). It is possible that process mining will serve a similar purpose in auditing research. This paper also opens a new avenue for research into how auditors can best make use of the population-based business process view that process mining promises. Brewster (2011) argues that "[a]uditing theorists suggest that training auditors to use systems-thinking skills can improve how they learn and use complex entity-level evidence that would normally overwhelm auditors... [This] suggests that new systems-based training methods could help auditors to learn better in the field and develop the skillsets needed to understand complex environments." Future research can examine whether process mining will help auditors achieve this objective.

Section II develops a protocol for applying process mining as an analytical procedure in auditing. Section III presents an overview of the field study. Section IV then applies the protocol for process mining of event logs in auditing developed in Section II to the field site data. It demonstrates the value added that process mining can provide to auditors when used as an analytical procedure to extract audit-relevant information from the event log. Section V discusses

the role of process mining in accounting research, and Section VI offers concluding comments. A link to an appendix provides a brief discussion of how to construct an event log.

II. A PROTOCOL FOR APPLYING PROCESS MINING AS AN ANALYTICAL PROCEDURE IN AUDITING

Most large businesses today store their structured data digitally in enterprise resource planning (ERP) systems, such as the SAP™ system used in this field study site. The data recorded by an ERP system includes not only entries made by users of that system, which we refer to as "input-data," but also "meta-data," which is information recorded automatically by the system about that input data. Meta-data includes the timestamp of transactions and the identity of the person entering the data. Such information is located in various tables throughout the ERP system's database, and, to create an event log, those data are extracted and assembled into a structured database that facilitates systematic analysis of the input and meta-data.

Basic IT security controls must be in place to preclude a user from overriding the automated logging of the event log data. Analytical procedures rely on the integrity of the underlying data, and this requirement is not unique to process mining. Four characteristics must be extracted from the information system about each event in order to enable process mining analysis:

1) the *activity* taking place during the event (for example, sign, authorize, pay);
2) the *process instance* of the event (for example, an invoice, a receipt, a purchase order);
3) the *originator*, or party responsible for the event; and
4) the *timestamp* of the event.[4]

At least some of these four characteristics are logged by ERP systems independent of the originator. Each user is required to log into the ERP system with a unique password before being able to enter a transaction and the system timestamps each data entry even if the originator also physically enters a date.

Once an event log is created, there are numerous tools available for analysis. Because process mining must satisfy cost/benefit criteria, the following protocol aims at focusing systematically on the transactions that warrant further audit investigation:

(1) Identify the Designed Process: Determine which activities need to be included in the event log.
(2) Event Log Creation: Because data storage architecture varies across ERP systems, event log creation is currently not an automated process. The event log that describes the designed process of interest must be developed using knowledge about how the particular ERP system operates, as well as how a given business chooses to handle its data. For example, most IT systems could record more meta-data than they actually do (at an extreme, actual keystrokes could be recorded), but such recording slows down the system. Nevertheless, many important insights can be obtained even when meta-data are restricted to the minimum that virtually any system records, the *Originator* and *Timestamp* variables. Conceivably, the nature and content of event logs could be standardized and configured within the ERP facilitating their analysis.[5]

---

[4] For example, the event with unique identifier 01340001 refers to a *Sign* (activity) of *Purchase Order 4603* (process instance) by *Ann Smith* (originator) on *October 5th 2012* (timestamp).

[5] The AICPA has been issuing Audit Data Standards (AICPA 2013) that provide guidance for data to be made available to the audit function that will facilitate the creation of event logs. http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/auditdatastandards percent20base percent20august2013.pdf (last accessed July 24, 2014).

(3) Process Discovery: The most important insights that process mining can provide involve using data contained in the event log to show how processes actually operate in a business.

Although processes are mostly prescribed to take place according to a designed process model, some room for flexibility is necessarily built into the business's ERP system. This flexibility is designed to allow for the numerous deviations from the designed process model that are often required in practice for smooth operation of the business, constraints that would otherwise interrupt the process flow too frequently. For example, while ideally there would be a three-way match between a purchase order, a goods receipt, and an invoice, an allowance may be made to accept deliveries that include unanticipated transportation costs that were not included in the original purchase order. Otherwise, such deliveries may be frequently rejected, resulting in unacceptable delays to the downstream production process. In today's heavily IT-enabled businesses, this flexibility is allowed in the ERP system, and, while IT internal auditors periodically check ERP system settings, they also anticipate that these settings will occasionally change to allow for exceptional transactions, cope with changes in personnel, etc. Hence, rigid internal controls are not practical, implying that monitoring only the internal controls over financial reporting (ICFR) is not sufficient to cover all the risks associated with the business process. Thus, the auditor has to anticipate that there will be deviations from the designed process, and he/she will have to use procedures to assess whether such deviations are acceptable or evidence of control failure. Process mining techniques show not only how processes actually operate, but also allow the auditor to focus on these specific deviations from the designed process that pose the greatest control risk.[6]

(4) Role Analysis: While process discovery identifies the business processes, role analysis focuses on the roles of individuals in the process. The *Originator* variable in the event log is one of the most important sources of value added that process mining offers to auditors because it identifies the auditee entering data into the ERP system. This enables the auditor to determine who took what action as far as transactions are concerned. Role analysis, as we show, also fits into the renewed attention that auditors have placed on segregation of duty (SOD) controls in the wake of Section 404.

(5) Attribute Analysis: The more data the event log provides the auditor about the actual activities being undertaken, the more it yields insights into inconsistencies between the discovered process and the designed process by pinpointing specific areas where violations are taking place. Instead of simply discovering processes, attribute analysis allows a more subtle examination of when flexibility in the control architecture is appropriate and when it has been abused.

(6) Social Network Analysis: Role analysis is used to examine anomalous transactions identified using process discovery and attribute analysis, triangulating on not only transactions that warrant investigation, but also on the employees involved. This is perhaps the area that warrants the most research relative to application of process mining because it offers the promise of allowing auditors to tackle the historically intractable problem of collusive fraud.

In this paper, the benchmark for success in the application of process mining to event logs is the detection of audit-relevant information. Thus, as Brewster (2011, emphasis added) states:

---

[6] Alternatively, the auditor could put in place systems to monitor and issue alerts when deviations take place from the designed process. In the bank examined in this case study, deviations were permitted of up to 2 percent of the difference between the purchase order and the actual invoice, with alerts issued otherwise. However, in terms of specifying the precise order of the activities, the process was quite loosely structured in order to be operationally effective. A major constraint is that such intrusive monitoring reduces the speed of the IT system.

"When performing analytical procedures, auditors should treat *any* discrepancies between pre-developed expectations and management representations as indicators of heightened misstatement risk."

III. FIELD STUDY SITE

The field study location is a leading European bank that ranks among the top 25 in the world by asset size. It is also subject to provisions of the Sarbanes-Oxley Act because of its operations in the United States. We focus on the bank's procurement process because it is a typical, standardized business process in most businesses around the world and, hence, makes the field study more generalizable. Moreover, procurement represents a large expense item, totaling some €1.4 billion in the period covered in this field study. Further, because it is a process with implications for the financial reporting process, it is subject to Section 404 controls under the Sarbanes-Oxley Act, particularly SOD controls.

The greatest hurdle of any field-based research involves gaining access to confidential firm data. Few businesses would allow outside researchers to examine very recent transactions, but contemporaneous information would not suit our purposes in any case because such data would not have been already audited. On the other hand, use of much older data limits the ability of internal auditors to effectively investigate any audit-relevant information that the process mining protocol uncovers. Further, this bank was severely affected by the global credit crisis that began in 2008, so data from that period lack generalizability. Given these constraints, we use data from 2005 to early 2007. This period was sufficiently before the credit crisis began, and still within the bank's internal auditors' institutional memory.

Data were available for the construction of event logs for this project because the bank uses SAP™ for its procurement cycle. The configuration settings of the ERP system are the focus of internal controls over financial reporting, and the procurement process over the field study time period had already been reviewed by the bank's internal auditors, who found no major issues of concern.

The transactions in the field study consist of all the invoices *paid* during the month of January 2007, which were then traced back to their accompanying purchase orders (POs). These POs had creation dates between 2005 and January 2007, and we followed them from their start activity, *Create PO,* to their end activity, *Pay*. If the end activity was not a single payment but rather consisted of multiple payments, then the ending activities were cut off after the last payment activity, with this final payment taking place in January 2007. Hence, the event log only contains completed procurement cycles, a choice that may restrict the types of anomalies that can be detected. Imposing this limit, however, prevents the issuance of false alarms attributable to incomplete procurement cycles materializing because POs are not yet associated with payments.

The process mining techniques facilitate analysis of the entire population of invoices paid in January 2007, in contrast to the sample examined by the bank's internal auditors, thereby demonstrating the ability of process mining techniques to evaluate a monthly population of transactions. Because the entire population of data is analyzed, the distinction between analytical procedures and tests of detail becomes moot. Process mining gives auditors the ability to dispense with sampling and analysis restricted to aggregated data.

A variety of research tools was used to obtain the necessary details about the procurement process. Clarification was obtained about processes from business and information systems specialists, employees in various departments, personal observation, and consultation of ERP system user guidelines. With that comprehensive view of the procurement process in hand, the protocol for process mining of event logs in auditing was implemented.
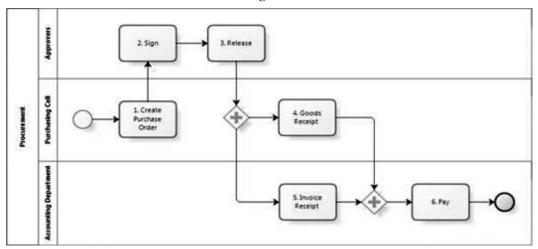
FIGURE 1
Flow Chart of the Designed Procurement Process

Source: Jans et al. (2011).

This figure provides an illustration of the procurement process in an ideal setting without any changes once the purchase order is created or any alterations made to the control system.

IV. IMPLEMENTING THE PROCESS MINING PROTOCOL

Identify the Designed Process

The flow chart in Figure 1 describes the main activities in the designed procurement process. The process starts with the creation of a *Purchase Order* (PO). This PO must be *Signed* and *Released* by two different and authorized employees, thereby approving the PO for release. Once the system releases the order, the employee can order the goods from the supplier.[7] The supplier will then dispatch the goods and the accompanying invoice. When both the *Goods Receipt* (*GR*) and *Invoice Receipt* (*IR*) are entered into the system, the accounts payable employee will book the invoice in the general ledger, which will trigger the *Pay* activity.

As discussed previously, for operational reasons the procurement process can vary from the designed model as shown in Figure 1. For example, changes can be made to the purchase order after it has been created, potentially requesting new approvals (*Sign* and *Release* activities). This extra activity (*Change PO*) is not an explicit part of the designed process model, but is added to the process model to capture these non-standard activities. Another example of a possible and plausible process variation pertains to the receipt of goods in multiple deliveries. This would cause extra activities of *Receive Goods,* and potentially additional activities of *Receive Invoice*.

In practice, therefore, process executions can deviate (sometimes frequently) from the designed process. This poses a serious question for the auditor because once primary controls are relaxed to allow deviations from the designed process, how can control be retained over that process? Aside from monitoring the installed controls, the auditor must analyze the deviations from the prescribed model, bearing in mind that not all exceptions are necessarily indications of internal control flaws.

---

[7] Because this takes place outside the ERP system the supplier activity is not depicted in Figure 1.

TABLE 1

Frequency of Activities in the Event Log

Activity	Absolute Frequency	Frequency Activity/ Frequency "*Create PO*"
1. *Create PO*	26,185	1.0000
2. *Sign*	25,648	0.9795
3. *Release*	28,748	1.0979
4. *GR*	24,724	0.9442
5. *IR*	29,255	1.1172
6. *Pay*	31,817	1.2151
Change Line	15,468	0.5907

Absolute frequency and relative frequency in relation to frequency of "*Create PO*" activity showing that not all activities take place only once as indicated in the designed process.

Some process deviations are normal, others are suboptimal, and still others are anomalous outliers that require further investigation. Hence, tests of details are required to supplement the tests of controls. Process mining can aid the auditor in conducting these tests of detail in a more comprehensive and systematic fashion, but this necessitates first creating the event log that captures all essential aspects of the designed business process.

Preliminary Analysis of the Event Log

Once the event log was created, a preliminary analysis was conducted to better understand the way in which purchasing was actually carried out in the bank. The event log consists of all data stored in the bank's ERP system relative to the 31,817 payments made in January 2007. Tracing back in time showed that these 31,817 payments were instigated by 26,185 process instances, which in this case are purchase orders issued by 272 distinct originators. Between their origins as POs and their conclusions as payments, these 26,185 purchase orders were subject to 181,845 distinct activities. The frequency of activities in the event log is summarized in Table 1. The number of process instances in the event log, 26,185, must equal the activity of *Create PO*, because this activity refers to the creation of the parent PO that this PO item line belongs to, and that activity is assigned to each PO line. If the designed procurement process is followed, then all activities should take place the same number of times. The fact that the number of activities is not the same provides immediate evidence that the actual process differs from the designed process, indicating either necessary flexibility to accommodate business needs or a failure in ICFR for each deviation.

Table 1 indicates that there are less *Sign* transactions than there are PO (lines) created, meaning that not every PO is signed. On the other hand, there are more *Releases* than PO lines. In addition, more payments are identified than cases, implying multiple payments on one PO line. Surprisingly, almost 60 percent of POs have changes.

The average completed procurement process instance consisted of six events, with a minimum of four and a maximum of 390. This maximum audit trail is likely an open order, one for which a single PO line is used over and over again. Nonetheless, it is clearly a transaction that warrants further investigation by the internal auditors. In short, even this preliminary analysis clearly indicates that there are many issues that need to be examined in detail. The first step in that systematic evaluation is process discovery.

Process Discovery

The most fundamental use of process mining is to analyze the event log in order to discover how the business process was actually carried out. The discovered processes can then be compared and contrasted with the designed process model, enabling the identification of deviations that have taken place due to the necessities of operations or the violation of controls. Process discovery is achieved by examining meta-data timestamps to systematically establish the flow of activities for each PO line, from creation to payment. This type of analysis is unique to process mining because it utilizes process-related data instead of only static transactional data. Using traditional analysis techniques would not yield these insights because they rely only on data entered by the auditee that cannot be compared with independent system information.

The first step in gaining insights in the process executions is to analyze the number of variants. A variant is a unique sequence of activities in the event log. For example "*Create PO → Sign → Release → GR → IR → Pay*" is a variant. It summarizes one way of executing the procurement process. A total of 304 different variants were identified in the case study with the six most frequent variants shown in Table 2. Whether 304 variants are more or less than what one might expect of a business of this size and complexity is an open question. There is currently no benchmark available from procurement or other business processes to serve as a basis of comparison.[8] Even in the absence of such a benchmark, the number and variety of ways in which the procurement process is being performed is surprising.

Table 2 indicates that just three out of 304 variants account for over 80 percent of the data set. By contrast, there are 104 variants that only occur once. Relating the six variants shown in Figure 1, the first entry is recognizable as the designed procurement process, but it encompasses under half of all process instances. Variant 2 differs from the designed process in that there is a change that takes place in the PO after it is created. However, this is not a major audit concern because the change takes place before the PO is approved.

By contrast, in variants 3 and 4 the *Sign* activity is absent altogether, contrary to specifications of the designed model. When these anomalies were brought to the attention of the bank's internal auditors, they stated that there are circumstances in which it is legitimate to *Release* a PO without a signature. For example, some senior managers may have authorization limits that allow the release of POs on their own authority. These exceptions and/or circumstances can be formalized and built into analytic tools.

In variants 3, 4, and 5, there is no *GR* document entered into the ERP system. This can happen legitimately when there is no act of product delivery to a shipping dock, as in the case of a cleaning service. The *GR* indicator should be flagged in the SAP™ system to indicate that no *GR* entry is to be expected in such a case, but possibly this action had been overlooked by originators. An auditor would likely want to investigate these variants to ensure that they do indeed represent services rather than goods, and that the services purchased are appropriate for the business. In the last variant, the order of the *IR* and *GR* are reversed. However, as depicted in Figure 1, the activities *IR* and *GR* are allowed to appear in parallel order that would explain this phenomenon.

If several of these six non-designed variants in Table 2 warrant some sort of further examination by internal auditors, then it is likely the remainder of the 304 process variants fall into this category as well. On the one hand, one could dismiss these 298 as insignificant, because they encompass less than 14 percent of all purchase orders. On the other hand, that rationale may be

---

[8] Analysis recently carried out of the procurement process at another business (by one of the co-authors) revealed well over 8,000 distinct variants. Much remains to be learned about the extent to which processes in practice can deviate from the designed process and the factors that determine the magnitude of those deviations.

TABLE 2

Most Frequent Variants in the Event Log Illustrating the Variety of Ways in Which the Actual Procurement Process Differs from the Designed Process

Variant #	Sequence	Variant Frequency		Cum. Total	Paid Value	Throughput Time (Days)			
		#	%	%	Euros	Avg.	Min	Max	Std. Dev.
1.	Create PO → Sign → Release → GR → IR → Pay	11,608	44.3%	44.3%	7,634,968.47	27.78	1	334	20.05
2.	Create PO → Change Line → Sign → Release → GR → IR → Pay	6,955	26.6%	70.9%	8,178,348.22	32.33	2	343	57.72
3.	Create PO → Change Line → Release → IR → Pay	2,488	9.5%	80.4%	504,341.51	75.63	3	344	38.99
4.	Create PO → Release → IR → Pay	640	2.4%	82.8%	176,540.63	16.8	3	338	26.38
5.	Create PO → Change Line → Sign → Release → IR → Pay	491	1.9%	84.7%	1,166,303.16	50.85	6	237	24.07
6.	Create PO → Change Line → Sign → Release → IR → GR → Pay	393	1.5%	86.2%	344,583.22	56.36	9	295	40.16

precisely why they should be of the greatest concern to internal auditors, because they represent outliers. Furthermore, these 298 items involve €40.4 million, a substantive amount.

Analyzing the remaining 298 variants would be a desirable extension of the current study and is the subject of ongoing research. The first step is to determine the variants that are acceptable deviations from the designed process—being dictated by the operational necessity—rather than by violations of control procedures. But the findings of this field study suggest why creating such a knowledge base through a more widespread application of process mining would be of value to auditors.

In the absence of a suitable benchmark, the discovered process variants are compared against each other by using a process discovery algorithm to analyze the sequence of activities within the audit trail. Given the extensive number of variants, some with a large number of activities (the maximum being 390), visual observation no longer suffices to examine all the audit trails. Hence, Disco, a commercial software tool, is used as part of the process mining analysis.[9]

Initially, the default setting of Disco, which is based on the Fuzzy Miner algorithm of Günther and van der Aalst (2007), is applied. It filters for the typical issues encountered with large real-life datasets and then simplifies and visualizes complex processes. Where the original Fuzzy Miner algorithm suffered from depicting activity flows that did not occur in the dataset, the algorithm of Disco eliminates these false outcomes. The application of this improved algorithm extends the work of Jans et al. (2011), where the Fuzzy Miner algorithm was applied. The output showing the most observed process models underlying the data are depicted in Figure 2. The darker the rectangle, the more frequently this activity is executed. The thicker the line, the more frequently this sequence of activities occurs. The core process shown corresponds to the designed process, reflecting the frequencies in Table 2. The deviations depicted are a *Change* that often occurs between the creation of the PO and the *Sign* activity as in variant 2 of Table 2. There is also some interaction between the payment and invoice receipt, which is established to be legitimate following discussions with process owners and internal auditors.

Using the default settings of this algorithm visualizes the most observed behavior in the event log. To uncover the less frequently followed paths, we lower the thresholds for the metrics in the algorithm, resulting in the model in Figure 3.

In Figure 3, a more complex process can be observed with extra flows (identifiable as *edges* to the core process). The extra flows (subsets of audit trails), along with their frequencies are summarized in Table 3.

In Table 3, sequences 1 and 2 are absent a *Sign* activity. Upon questioning the bank's process experts, it was established that there are situations where a stand-alone release suffices as approval, but only when additional conditions are met (in this case: a maximum amount should not be exceeded and a specific document type had to be used). To test these business rules, these conditions will be tested in the attribute verification phase of process mining.
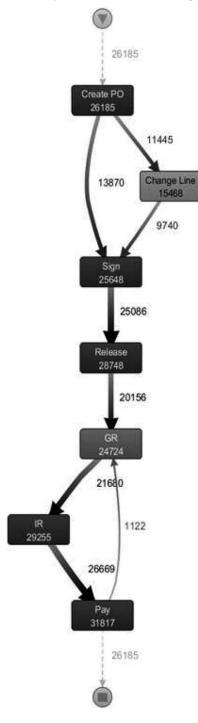
There are also 19 cases where a *Sign* event was immediately followed by a *GR*. This is in violation of ICFR whereby a *GR* can only be executed after a release. While these cases were found to be legitimate upon further investigation, process mining succeeded in discovering flows that warranted investigation by the internal auditors.

To put the *Sign* and *GR* activities in context, it is important to understand the different underlying data structures. A *Sign* (and also a *Release*) relates to an entire PO. A *GR* on the other hand, only relates to a specific item line. This different data structure is the underlying cause for some discovered process flows. In the 19 cases where *GR* directly followed after *Sign,* the *Sign* activities were all related to a change that took place in another item line, different from the
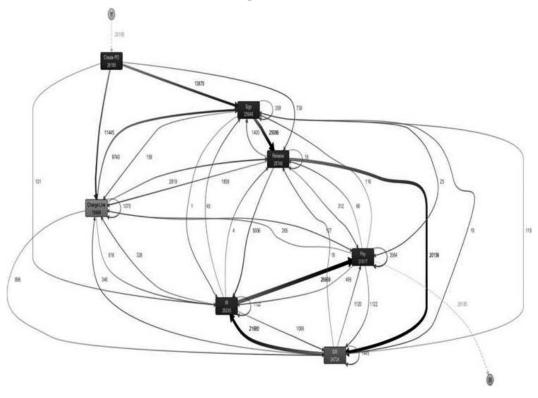
---

[9] http://www.fluxicon.com/disco

FIGURE 2
Output of Disco Fuzzy Miner Analysis with Default Settings to Uncover Core Processes

This figure provides an illustration of the most commonly occurring steps actually taking place in the procurement process.

FIGURE 3
Output of Disco Fuzzy Miner Analysis with Lower Threshold Setting to Reveal Less-Frequent Flows

This figure provides an illustration of both the most commonly occurring steps taking place in the procurement process as well as less frequent flows.

process instance itself. The *GR* activity was not associated with the *Sign* that took place just before the *GR*.

The fourth and fifth extra flows, *Release → IR* and *Release → Pay,* both stress the importance of the *GR* indicator. The business makes it permissible to discard the *GR* activity in the case of a service, as described previously, but the *GR* indicator was supposed to have been turned off in those

TABLE 3
Results of Explicit Checks on the Extra Edges in the Fuzzy Miner Output Illustrating the Frequency with Which Certain Anomalous Sequences Occur

Seq.	Extra Flows	Occurrences	Result
1.	*Create PO → Release*	739	Verification required for omitting *Sign*
2.	*Change Line → Release*	2,819	Verification required for omitting *Sign*
3.	*Sign → GR*	19	Further investigation → OK
4.	*Release → IR*	5,006	Verification required on *GR* indicator
5.	*Release → Pay*	312	Verification required on *GR* indicator and *IR*
6.	*Pay → IR*	499	Verification required on *IR*

circumstances. Whether this procedure was complied with will be examined during the verification phase.

Variants 5 and 6 in Table 3 stress the importance of testing whether for each payment there exists a matching invoice. This too had to be checked using attribute verification in the next stage in the process mining protocol. Finally, we examined whether each PO had minimum one *Release* in its flow. Three cases out of the population of 26,185 were found to have no such release. On two occasions, this was attributable to a PO that was created by a batch file, paid, and subsequently reversed, but these transactions managed to make their way through the procurement process without an approval, which is clearly a cause for concern. In the third case, further investigation revealed that the approval actually took place outside the ERP workflow, which is why the release was not explicitly recorded in the event log.

There is more analysis that could be conducted relative to these variants. For instance, throughput time data shown in Table 2 could be incorporated into the evaluation. However, the aim of this paper is not the comprehensive examination of this particular event log, but, rather, to establish that there is value added to process mining in auditing. Clearly, even these limited process discovery tasks revealed numerous examples of audit-relevant information that warrant further investigation by internal auditors. Next, other process mining tasks are undertaken to better define the potential contribution of process mining to auditors.

Role Analysis

Role analysis exploits the presence of meta-data on activities and originators in the event log to examine the parts played by employees in the procurement process. In order to satisfy Section 404 of the Sarbanes-Oxley Act, businesses have instituted many additional preventive controls for segregation of duties (SOD). Their aim is to ensure that the same individual is not responsible for all critical steps in a process, such as both creating and signing POs. However, because individuals often execute several activities, they can have multiple roles in overlapping processes. In addition, the inherent flexibility in ERP systems can lead to slippages in control over time as personnel change their employment status and/or roles. Hence, in addition to test of controls, there is also a need for tests of detail to ensure that SOD rules are not being violated in the procurement process.

In this case study, the bank has three SOD controls:

(1) The *Sign* and *Release* activities for a given PO should be undertaken by two distinct individuals.
(2) The *GR* and *IR* activities for a given PO should be undertaken by two distinct individuals.
(3) The *Release* and *GR* activities for a given PO should be undertaken by two distinct individuals.

The first step in undertaking role analysis is to use the data in the event log to create an Originator-Task matrix that details the number of times an individual executes a particular activity. The matrix enables a preliminary check to be conducted to determine whether an individual executes an impermissible double role. With 272 originators in this field study, the full table is too large to show. However, from the excerpt presented in Table 4 it is found, for example, that individual "...,1" undertakes both the *Sign* and the *Release* activities. Similarly, individual "...,4" initiates both *GR* and *Release*. No example of an individual combining the *GR* and *IR* roles is found in the matrix.

The matrix provides only a preliminary analysis because it only shows total activities and activities isolated by the process instance. Thus, the 11 cases that individual "...,1" released may or may not coincide with the 171 that he or she signed, and there is obviously no violation of SOD controls if the 11 released cases are different from the 171 signed cases. The situation could simply

TABLE 4

Excerpt of Originator-Task Matrix Showing
Which Individual Undertook Which Activity

Originator	1. *Create PO*	2. *Sign*	3. *Release*	4. *GR*	5. *IR*	6. *Pay*	Change Line
…1							
…2	0	171	11	0	0	0	0
…2	0	0	0	0	280	310	0
…3	0	0	23	0	0	0	0
…4	0	0	42	42	0	0	0
…5	0	24	0	0	0	0	0
…6	152	0	0	189	0	0	204
…7	0	0	10	0	0	0	0
…8	0	0	66	0	0	0	0
…9	0	0	1	0	0	0	0
…10	207	241	0	199	0	0	155
…11	0	0	0	15	0	0	11
…12	4,572	259	0	4,517	0	0	244
…13	…	…	…	…	…	…	…

reflect a reassignment of responsibilities, perhaps due to a promotion of the individual involved, or the need to temporarily replace an absent colleague in the *Sign* role. Hence, identifying individuals with combined roles only highlights audit-relevant information that warrants further investigation by the internal auditors. However, the tools of process mining enable the SOD controls to be tested comprehensively on the population of data and for a period in time (versus a certain point in time).

Given the size of the Originator-Task matrix in this case, visual inspection cannot be used to detect all suspect SOD instances. A Linear Temporal Logic tool can be used to check whether the three fundamental SOD controls given above hold for originator of the POs. This tool tests the population of data, on a case-by-case basis, against these rules. It determines whether individual originators exert their authorization on multiple activities on single purchases, thereby violating the principles of segregation of duty.

The first assertion—that *Sign* and subsequent *Release* of a PO are by two distinct individuals—needs to be tested in a pairwise manner, because there can be multiple signs and releases for one process instance. Although this scenario should not occur in the designed process, there are numerous variations and loops that might be exhibited in the actual process. For instance, if a *Sign* and *Release* take place and then a line is subsequently changed, the next *Sign* is allowed by the bank to be performed by the former releaser. The control test in this case needs to check whether the *Release* next to the last *Sign* is executed by someone other than the person who signed the altered PO.

After testing the entire population of 26,185 POs, it was concluded that the first two SOD controls hold without any violation in the investigated event log. The fact that an auditor could make such a clear-cut assertion as to the efficacy of these two SOD controls for the entire population of transactions across all company personnel is itself indicative of the value added that process mining provides in auditing.

For the third assertion, however, 175 violations were found involving three originators. One of these three employees violated the SOD control on *GR* and *Release* 129 times, another incurred 42 violations, while the third person did so four times. These 175 cases revealed by the role analysis

task are clearly audit-relevant information, and this is a further demonstration of the value of role analysis in auditing.

Verification by Attribute Analysis

Applying the first two components of the process mining protocol to the field study event log yields numerous outcomes that warrant further investigation to assess whether they represent violations of controls. Portions of this investigation must be undertaken manually by the internal auditors, but, in some cases, it can be done by using other process mining tools that exploit the information on attributes of the process instances available in the event log.

An attribute contains characteristics of the executed activity or characteristics of the process instance itself (here the PO). The following analyses are selected from a broad array of possible checks. The output of the activity variants found in the process discovery and role analysis components of the process mining protocol are used as input to make a selection for further verification analysis. Using software, we first compare the references of the payment to the invoice references to check whether there is an accompanying invoice for each booked payment. These references are examples of attributes that are stored in the event log. This test resulted in 46 incorrect process instances encompassing 265 payments. One process instance had 131 pay activities without a corresponding invoice; another instance contained 75 payments without invoice. A third process instance has ten payment activities without invoice. The remaining process instances only have one, two, or three stand-alone payments. There were 17 employees involved in these payments. One of these persons is accountable for 216 out of the 265 payments. Two other individuals have 18 and 12 standalone payments, respectively, on their accounts. These payments were all investigated by the bank's internal auditors to check whether the payments are based on a different type of document (*Subsequent Debit*), an acceptable alternative. This indeed appears to be the case with all of these payments. The question remains as to why these payments are allowed to be based on this type of document instead of a regular invoice.

The second analysis follows up the revealed variants in the process discovery task by investigating the functioning of the *GR* indicator. The designed function of this indicator is that invoices can get paid while no goods were received at that moment. In that case, the indicator should be turned off. It was tested as to whether all paid cases without a *GR* indeed had a *GR* indicator that was turned off. Three cases were identified where this assertion did not hold, indicating a breach in the configuration settings of the ERP system. As discussed above, in this context, it would be useful to have an attribute for whether this case refers to services or goods. That there is no such field in the bank's SAP™ system is a shortcoming in the ICFR as revealed by process mining.

The last attribute analysis verifies whether the internal conditions of the organization are met when there is no *Sign* in the variant. There were 742 cases (2.8 percent of the total) that both lacked a *Sign* activity and failed to meet the conditions under ICFR for which such an omission is permissible. This evidence was handed over to the internal auditors for follow-up investigation, but, for reasons of confidentiality, they could not or would not share the outcome of those inquiries.

Social Network Analysis

The *originator* entry in the event log enables us to construct a social network demonstrating all the interactions between the employees involved in the procurement process. The social network of all the employees is depicted in Figure 4, with each circle representing one out of the 272 individuals in our population. The range of interactions between such a large number of employees
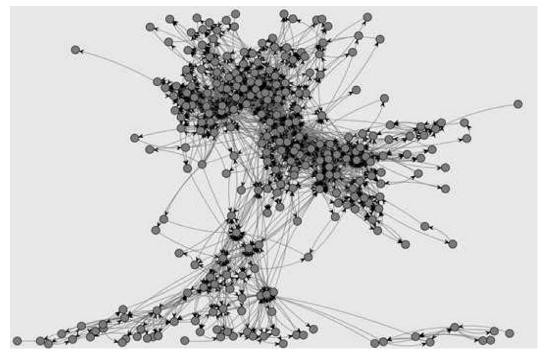
FIGURE 4
Social Network of All Originators in the Procurement Process

This figure provides an illustration of the degree of interaction between the 272 distinct individuals taking part in the process.

results in output from which it is difficult to gain much insight. In fact, social network analysis has proven most valuable when it can be focused on a specific subgroup of interest.
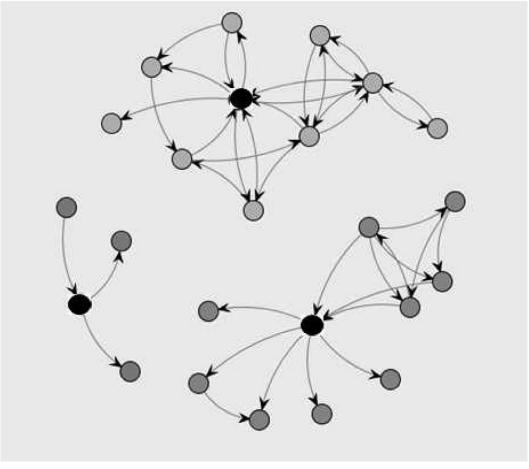
Thus, a social analysis was undertaken of the subgroup of 175 cases involving the three individuals identified by role analysis to be in violation of the SOD control concerning the *Release* and *GR* activities. The analysis centers on the three originators directly responsible for the violation, and maps that other employees interacted with them in the event log.

In total, 21 other individuals were involved with the three primary originators across the 175 cases. The social network of these 24 individuals is depicted in Figure 5. There are three distinct clusters, with the three individuals violating the segregation of duty controls shown in the central position of each cluster (these three employees are identified by the filled black circles: •). This map of their social networks provides the opportunity to compare the designed organizational structure with the actual network.

Another interesting subgroup is the social network of individuals involved with the 742 cases identified by attribute analysis where no *Sign* was present and the conditions for this exception were not met. As before, a social network diagram is constructed by using the originator entries in the event log cross-referenced against the 742 process instances. Figure 6 shows this social network, and indicates that there are three clusters of employees, with two of the clusters connected to each other by two individuals who are involved with both groups. By contrast, the third group is both completely isolated and involves only three individuals. Given the small number of employees in this cluster, one possibility is that this is an instance of people in an office sharing passwords to

FIGURE 5
Social Network of 175 Cases by Three Individuals Violating SOD Controls on *Release* and
GR

This figure provides an illustration of who else these individuals interacted with while undertaking those transactions.

access the ERP system: a violation of security controls, but an all-too-frequently occurring problem. Isolating the users through process mining facilitates the verification of this hypothesis.[10]

A social network analysis is not an end in itself, but a means toward obtaining insights into the meaning and motivation of transactions through understanding how the individuals involved relate to each other in an organization. Social network analysis may be a way of tackling collusive fraud. The clusters shown in Figures 5 and 6 are not evidence by themselves of fraud, but limit the scope of follow-up internal audit investigation to a manageable subset of all employees. The real value added arises when social network analysis is combined with other process mining tasks, such as

---

[10] Section V discusses another verification check that can be carried out on this result.
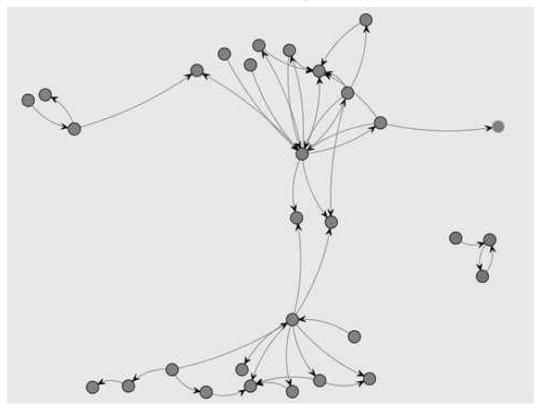
FIGURE 6
Social Network of the 742 Cases without *Sign* and in Violation of Controls

Source: Jans et al. (2011).
The figure illustrates which individuals were involved in those transactions and who else they interacted with.

process discovery and attribute analysis. This exploits the full dimensionality of the data in the event log, and focuses attention on the most serious violations of controls.

V. RESEARCH IMPLICATIONS OF PROCESS MINING

Process mining is a different approach to auditing: it focuses on the path of transactions and not directly on the validation of its values, and uses the full population of data instead of a sample of that data. As with any analytical procedure, process mining can create problems of its own as the number of exceptions generated in the examination of a large sample can be overwhelming and methods of identifying "exceptional exceptions" (Issa 2013) must then be developed.

To mitigate the problem of an "alarm flood," process mining can be used in conjunction with other analytical procedures to narrow down the audit investigation. In the case discussed in this paper, transactions already identified as suspect by the social network analysis capabilities of process mining, such as the cluster of three employees in Figure 6, would have a higher suspicion loading. Benford's Law is a widely used tool by internal and external auditors to distinguish manufactured numbers from those originating naturally (Durtschi, Hillison, and Pacini 2004;

Nigrini 2012). Hence—assuming sufficient data were available to make the test feasible—all the transactions of these three employees could be subjected to a Benford's Law analysis to determine if the transactions that all three undertook together stand out as not being the result of the normal procurement process. In this way, it would be possible to validate whether the audit-relevant information generated by process mining is really indicative of fraud, while avoiding having to deal with a flood of false positives that would arise when any analytical procedures are applied to the entire population of data. More research is needed on the optimal use of process mining in conjunction with existing analytical procedures.

An important effect of process mining entails extending the domain of auditing from only transactional data entered by the auditee to meta-data automatically and independently recorded by the IT system that describes the process that gave rise to those transactions. We are only in the formative stages of understanding how auditing practice will change when it exploits meta-data (Jans et al. 2013).

The issue of the existence of audit standards and the emergence of new analytic technologies has been discussed by Titera (2013) who states: "Audit Standards inhibit the external auditors' use of enhanced data analysis and continuous auditing techniques." The results of this field study indicate that process mining may be a valuable tool in auditing practice. The conditions of its best usage in auditing need to be researched: whether process mining serves as a complement or substitute for existing analytical procedures; tailoring the process mining protocol to suit particular audit environments; and specifics concerning finer filtering of exceptions. A critical issue that also has to be investigated is the best way of rolling out such a sophisticated data analysis technique in audit practice.

Process mining is maturing, given the development of methods and software, to the stage where it will soon be a feasible tool for audit practitioners. It is still difficult for audit researchers to create event logs, but the tools to process mine data once obtained are readily and cheaply available. Once the first bottleneck is overcome, as it likely will be once ERP manufacturers see a demand for automatic generation of event logs, then audit researchers will be in a position to add process mining to the existing array of available analytical procedures.

The limitation of field study research is its potential lack of generalizability, but that is an issue only for results specific to the bank and not for the general conclusion that process mining can find audit-relevant issues that standard analytical procedures cannot. Because the data analyzed in this study were drawn from a routine process common to all other businesses, there is little reason to imagine that the value added of process mining would be substantially different with a different sample drawn from a different business. The results of this paper indicate that further research into the application of process mining in the audit domain needs to be undertaken, both to confirm the conclusions and to provide benchmarks to internal auditors for their own process analysis. Key questions to be asked include:

(1) How should process mining integrate with traditional audit analytic procedures?
(2) How can process mining be automated in order to facilitate assurance being undertaken closer to the time of the actual transaction?
(3) How should audit guidance and standards change with process mining?
(4) Where in the audit process should these be used?
(5) What are the behavioral issues in human judgment that need to be considered in the examination of process-mining-related technologies such as process discovery, role analysis, and social network analysis?

An entire new set of questions can also arise from the information theoretic standpoint, audit theory perspective, and practice implementation process. In the absence of further research, it is premature to conclude that process mining will have the same impact on the accounting literature,

but, certainly, the potential is there for it to open up entirely new domains for audit researchers to explore and formulate new questions to examine.

VI. CONCLUSION

The purpose of this paper was to establish whether process mining can add value to auditors as an addition to their analytical procedures toolkit. This field study had the advantage of having access to data previously audited by the business's internal auditors, thus providing a benchmark for assessing the incremental contribution of process mining in uncovering audit-relevant information not detected by standard audit procedures.

The bank's internal auditors did not find any significant ICFR weaknesses with the procurement process, and judged that its SAP™ controls were appropriately set to ensure a strong control environment. By contrast, the process mining analysis identified numerous instances of audit-relevant information that warranted follow-up manual investigation by the internal auditors under SAS 56:

(1) Purchase control procedures require *Sign* and *Release* for each purchase order, but the process mining analysis detected three POs that lacked these activities.
(2) SOD control procedures require *GR* and *Release* not to be undertaken by the same employee, but the process mining analysis detected 175 violations of this control.
(3) The process mining analysis detected 265 payments that lacked a matching invoice.
(4) The process mining analysis detected three POs that lacked a *GR* entry in the system, although the *GR* indicator was flagged.
(5) Purchase control procedures require a *Sign* activity in all cases except when certain exceptional circumstances occur, but the process mining analysis detected 742 occurrences where a *Sign* activity was lacking even though the conditions for this exception were not met.

These results can be attributed to two distinct differences/advantages of process mining over the standard audit procedures used by the internal auditors:

(1) the richness of the event log, which contains input and meta-data as well as a comprehensive set of attributes and its systematic arrangement by time and originator.
(2) the ability to analyze the entire population instead of being forced to use only a sample.

The identified ICFR issues represented only a small fraction of the total population, but that by itself does not indicate a reduced value to internal auditing because SAS 56 explicitly requires auditors to search for and investigate outliers, as these items are the most likely indicators of fraud and other control problems. Moreover, the fact that anomalous transactions are rare demonstrates the power of process mining, particularly when considering that the standard audit procedures failed to detect any of these issues.

REFERENCES

Agrawal, R., D. Gunopulos, and F. Leymann. 1998. Mining process models from workflow logs. In *Advances in Database Technology—EDBT '98*, edited by H. Schek, G. Alonso, F. Saltor, and I. Ramos. Berlin/Heidelberg, Germany: Springer.

American Institute of Certified Public Accountants (AICPA). 2013. *Base Standard*. New York, NY: AICPA Assurance Services Executive Committee Emerging Assurance Technologies Task Force.

Biggs, S., T. Mock, and P. Watkins. 1988. Auditors' use of analytical review in audit program design. *The Accounting Review* 63 (January): 148–161.

Bozkaya, M., J. Gabriels, and J. van der Werf. 2009. Process diagnostics: A method based on process mining. Paper read at the International Conference on Information, Process, and Knowledge Management (eKNOW), February 1–7, Cancun, Mexico.

Brewster, B. 2011. How a systems perspective improves knowledge acquisition and performance in analytical procedures. *The Accounting Review* 86 (3): 915–943.

Carpenter, T. 2007. Audit team brainstorming, fraud risk identification, and fraud risk assessment: Implications of SAS No. 99. *The Accounting Review* 82 (5): 1119–1140.

de Medeiros, A., A. Weijters, and W. Aalst. 2006. Genetic process mining: A basic approach and its challenges. *Business Process Management Workshops* 3812: 203–215.

Durtschi, C., W. Hillison, and C. Pacini. 2004. The effective use of Benford's Law to assist in detecting fraud in accounting data. *Journal of Forensic Accounting* 5: 17–34.

Folino, F., G. Greco, A. Guzzo, and L. Pontieri. 2009. Discovering multi-perspective process models: The case of loosely-structured processes. In *Enterprise Information Systems-B,* edited by J. Filipe, and J. Cordeiro. Berlin, Germany: Springer-Verlag.

Greco, G., A. Guzzo, L. Pontieri, and D. Saccà. 2006. Discovering expressive process models by Clustering Log Traces. *IEEE Transactions on Knowledge and Data Engineering* 18 (8): 1010–1027.

Gunther, C. W., and W. van der Aalst. 2007. Fuzzy mining—Adaptive process simplification based on multi-perspective metrics. In *Business Process Management, Proceedings*, edited by G. Alonso, P. Dadam, and M. Rosemann. Berlin, Germany: Springer-Verlag.

Hirst, E., and L. Koonce. 1996. Audit analytical procedures: A field investigation. *Contemporary Accounting Research* 13 (2): Fall.

Hylas, R., and R. Ashton. 1982. Audit detection of financial statement errors. *The Accounting Review* 57 (4): 751–65.

Issa, H. 2013. *Exceptional Exceptions*. Ph.D. dissertation, Rutgers Business School, Newark, NJ.

Jans, M. 2009. *Internal Fraud Risk Reduction by Data Mining and Process Mining: Framework and Case Study* (Ph.D. Thesis). Diepenbeek, Belgium: Hasselt University.

Jans, M., N. Lybaert, and K. Vanhoof. 2010. Internal fraud risk reduction: Results of a data mining field study. *International Journal of Accounting Information Systems* 11 (1): 17–41.

Jans, M., B. Depaire, and K. Vanhoof. 2011. Does process mining add to internal auditing? An experience report. In *Enterprise, Business-Process and Information Systems Modeling: 12th International Conference, BPMDS 2011, and 16th International Conference, EMMSAD, Proceedings*, held at CAiSE 2011, London, U.K., June 20–21, edited by T. Halpin, S. Nurcan, J. Krogstie, P. Soffer, E. Proper, R. Schmidt, and I. Bider. *Lecture Notes in Business Information Processing* (81): 31–45.

Jans, M., M. Alles, and M. Vasarhelyi. 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.

Kinney, W. 1987. Attention-directing analytical review using accounting ratios: A case study. *Auditing: A Journal of Practice & Theory* 6 (2) (Spring), 59–73.

Knechel, R. 1988. The effect of statistical analytical review on overall audit effectiveness: A simulation analysis. *The Accounting Review* (January) 74–95.

Li, F. 2010. Textual analysis of corporate disclosures: A survey of the literature. *Journal of Accounting Literature* 29:143–165.

Loebbecke, J., and P. Steinbart. 1987. An investigation of the use of preliminary analytical review to provide substantive audit evidence. *Auditing: A Journal of Practice & Theory* 6 (2): 74–89.

Nigrini, M. 2012. *Benford's Law: Applications for Forensic Accounting, Auditing, and Fraud Detection*. New York, NY: John Wiley & Sons.

O'Donnell, E., and J. Schultz, Jr. 2003. The influence of business-process-focused audit support software on analytical procedures judgments. *Auditing: A Journal of Practice & Theory* 22 (2): 265–279.

O'Donnell, E., and J. Schultz, Jr. 2005. The halo effect in business risk audits: Can strategic risk assessment bias auditor judgment about accounting details? *The Accounting Review* 80 (3): 921–939.

Peecher, M., M. Piercey, J. Rich, and R. Tubbs. 2010. The effects of a supervisor's active intervention in subordinates' judgments, directional goals, and perceived technical knowledge advantage on audit team judgments. *The Accounting Review* 85 (5): 1763–1786.

Public Company Accounting Oversight Board (PCAOB). 2010. *Substantive Analytical Procedures*. Washington DC: Public Company Accounting Oversight Board. Available at: http://pcaobus.org/Standards/Auditing/Pages/AU329.aspx.

Rozinat, A., and W. van der Aalst. 2008. Conformance checking of processes based on monitoring real behavior. *Information Systems* 33 (1): 64–95.

Titera, W. R. 2013. Updating audit standards—Enabling audit data analysis. *Journal of Information Systems* 27 (1): 325–331.

van der Aalst, W., B. van Dongen, J. Herbst, L. Maruster, G. Schimm, and A. Weijters. 2003. Workflow mining: A survey of issues and approaches. *Data and Knowledge Engineering* 47 (2): 237–267.

van der Aalst, W., K. van Hee, J. van Werf, and M. Verdonk. 2010. Auditing 2.0: Using process mining to support tomorrow's auditor. *Computer* 43 (3): 90–93.

van der Aalst, W. 2011. *Process Mining: Discovery, Conformance and Enhancement of Business Processes*. Berlin/Heidelberg, Germany: Springer-Verlag.

van der Aalst, W. M. P., M. H. Schonenberg, and M. Song. 2011. Time prediction based on process mining. *Information Systems* 36 (2): 450–475.

van Dongen, B., A. de Medeiros, H. Verbeek, A. Weijters, and W. van der Aalst. 2005. The ProM Framework: A new era in process mining tool support. In *Applications and Theory of Petri Nets 2005*, edited by G. Ciardo, and P. Darondeau. Berlin/Heidelberg, Germany: Springer.

Wilks, T. 2002. Predecisional distortion of evidence as a consequence of real-time audit review. *The Accounting Review* 77 (1): 51–71.

Wright, A., and R. Ashton. 1989. Identifying audit adjustments with attention-directing procedures. *The Accounting Review* 64 (4): 710–728.