Fraud Prediction and the Human Factor: 
An Approach to Include Human Behavior in an Automated Fraud Audit

Stefan Hoyer  
Leibniz Universität Hannover  
hoyer@iwi.uni-hannover.de

Halyna Zakhariya  
Leibniz Universität Hannover  
zakhariya@iwi.uni-hannover.de

Thorben Sandner  
Leibniz Universität Hannover  
sandner@iwi.uni-hannover.de

Michael H. Breitner  
Leibniz Universität Hannover  
breitner@iwi.uni-hannover.de

Abstract

Every year, fraud as a subset of insider threats causes billions US dollar of damage worldwide. We suggest a generic architectural model to unify the classic fraud audit approach with human behavior taking into account the fraud triangle in order to achieve better fraud detection and prevention. The human factor is extensively integrated into the audit as a qualitative component, in addition to the classic quantitative analysis of business transactions that are already being applied as part of the fraud audit. This provides added value because transactions examined by the auditor can be better differentiated and prioritized. It is possible to uncover transactions that are part of a pattern that is not yet known and that would have been left undiscovered using normal means by taking suspicious and non-suspicious human behavior into account. The proposed architecture is implemented using a prototype and is applied exemplary to an SAP ERP system.

1. Introduction

A current study from the Association of Certified Fraud Examiners (ACFE) demonstrates that fraud is a big problem in organizations [1]. The ACFE estimates that fraud causes a mean loss of 5% of the annual turnover of a company. The average fraud case runs at $160,000 in damages. A global study by PricewaterhouseCoopers showed also that such cases are quite widespread [2]. They found that 30% of the companies they surveyed had already dealt with fraud. Eighty percent of fraud is committed within the company's own ranks, especially in accounting, operations, sales, executive/upper management, customer service or purchasing [1]. The processes of the departments listed above are core elements of an accounting information system (AIS), which is of special importance for a fraud audit. Due to the high number of fraud cases, we are especially focusing on internal fraud audits.

Various methods and techniques for fighting insider threats, especially fraud, have been developed. In the past few decades, the focus was on developing technical instruments to examine information systems [3]. More recently, processes are taken into account [4]. Audit techniques have developed over time into continuous audit and real-time audit approaches. Despite these technical improvements, it takes an average of up to eighteen months to uncover a case of fraud [1]. From this we can conclude that the information provided by the current techniques is not necessarily sufficient to uncover a fraud case in a timely manner. As noted by Jans et al.: “Most important of all for auditing, there are anomalies or frauds that cannot be captured by analyzing input data alone” [5]. When referring to the triangle of people, process, and technology [6], the human factor appears to have been neglected. When taking the occurrence of fraud into account, including human behavior in the context of business processes has high potential. When we look at behavior, we can draw conclusions based on the three factors of the fraud triangle: incentives, opportunities und rationalizations [7].

We are introducing a generic architectural model that attempts to adequately consider the fraud triangle factors. In this way, in addition to the classic quantitative analysis of business transactions that are already being applied as part of the fraud audit, the human factor is extensively integrated into the audit as a qualitative component. This becomes clear when we look at the Enron financial scandal, which led to legal changes and tightening of legal regulations, such as the Sarbanes-Oxley Act (SOX). In the Enron employee e-mails published by the Federal Energy Regulatory Commission, there is evidence of inappropriate employee behavior [8] [9]. Holton introduces a process
that uses automatic e-mail text mining to detect similar circumstances [10].

Taking the human factor into account provides added value because transactions examined by the auditor can be better differentiated and prioritized. By distinguishing between types of behavior (suspicious and non-suspicious), it is possible to uncover transactions that are part of a pattern that is not yet known and that would have been left undiscovered if using normal means. Because fraud takes place using both known and unknown patterns, it is necessary to analyze the entire data pool during an investigation. Especially during a continuous audit, the focus of these types of audit can be determined and the circumstances that appear to be the most relevant can be prioritized.

In information systems (IS), there are two basic research approaches: behavioral science and design science. We are using design science methods described by Hevner et al. [11] [12]. Within this context we are following the design science research process (DSRP) model from Peffers et al. [13] [14]. An artifact in the form of a generic architectural model was developed in a solution-oriented way. This artifact has been pre-implemented as an early prototype within a test environment of a SAP enterprise resource planning system (SAP ERP). Iterations back to design have been performed using the review feedback and legal/ethical considerations of two certified information systems auditors (CISA).

The remainder of the paper is structured as follows. Section 2 gives an overview of related work. In section 3 and section 4 short basics of fraud, the well known fraud triangle and continuous auditing are given. Section 5 gives a risk oriented determination of the data population. Our generic architectural model, presented in section 6, is processed by an implementation of a prototype in section 7. We proceed with a discussion in section 8 and conclude with future work in section 9.

2. Literature review and status quo

There are papers in the literature that deal with the topic of recognizing the circumstances surrounding fraud or identifying people who could be involved in fraud. One of the most extensive overviews of automated fraud detection was done by Phua et al. [4]. They compared and summarized publications over a period of ten years. A briefer but more current overview was provided by Jans et al. as part of their work [15]. The identification and classification of potential fraud by suspicious people is a core element of the insider threat prediction model from Kandias et al. [16]. Like the approach described here, they used data from the IT infrastructure (e.g. intrusion detection system) to get an overview of users. The key aspect lies in classifying a person, but there is no further linking of results.

Jans et al. focused on reducing internal fraud risk by a descriptive data mining strategy of procurement data [17]. The evaluation of results was made through assessment of the data mining issues by domain experts. An automated risk rating was not implemented. They explicitly excluded the factors rationalization and incentive of the fraud triangle. The human factor is therefore not integrated directly. It is restricted to the analysis of business transactions.

In the topic of continuous auditing, there was a research focus on examining restrictions, improvements, and feasibility studies of the prevailing technical methods [18]. Kogan et al. analyzed continuous audit used for real-time error correction [19]. They used analytical processes to identify possible business process issues. The human factor and possible fraud-related behavior were not considered.

As fraud is a subset of the insider threat problem, we reviewed therefore also papers concerning insider threat prediction and detection.

Greitzer et al. [20] presented an approach that includes a combination of traditional workstation monitoring using cyber data and psychosocial indicators designed and weighted by human resource (HR) experts in order to predict an insider thread. Bishop et al. [21] provided an enterprise-level solution with the goal of getting early warning. Using HR and security database but also information about prioritization of assets and users who have an access to these assets, the insider attacks can be predicted. In addition to the psychosocial indicators as Greitzer et al. [20] proposed, Bishop et al. [21] used different communication entries (e.g. emails, blog) to analyze language affectation and afterwards to conclude additional threat rating information. As a result users were listed according to their risk level. Hence security personnel can concentrate its monitoring activity and HR staff can trigger counteractive measures on users with the highest threat.

Bishop et al. [22] investigated a threat problem analyzing different degrees of access and associated users. Examination of psychological indicators provides additional information about user risk level. Both Greitzer et al. [20] [23] and Bishop et al. [21] [22] accentuated the need of prediction solution instead of (or additionally to) detecting threats after they have already taken place.

We suggest unifying the classic fraud audit approach with human behavior taking into account the fraud triangle in order to achieve better fraud detection and prevention.
3. The nature of fraud

When we talk about fraud we need to talk about insider threat first. “The insider threat is manifested when human behavior departs from compliance with established policies, regardless of whether it results from malice or a disregard for security policies.” [20] Thereby fraud is one of the possible malicious actions adjacent to e.g. copyright contravention or illegal use of sensitive data. [20]

Fraud is a subset of insider threats. We here only consider financial fraud, which is committed by active insiders (for example male/female clerks, lower-level, non-technical positions). These insiders are still under direct control of the company (conceivable and possible activities are, for example, monitoring or the evaluation of personality traits) [24].

There is no general scientific definition of fraud. In principle, an auditor understands fraud to include all intentional actions of employees or third parties with the objective of attaining unfair advantage over the organization by illegal means (theft or modification for financial gain). This can be done, for example, through deception and misappropriation of assets and breaking the law. The ACFE defines fraud as: “The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.” [1]

With the ACFE definition in mind, the objective of our work is “...the category of fraud — occupational fraud — in which an employee abuses his or her position within the organization for personal gain” [1]. Fraud can be classified into corruption, asset misappropriation, and fraudulent statements [1]. Here we consider only the occurrence of fraud in which the ERP/AIS systems are used (business transactions such as accounting, orders or payments). Beyond the focus of this paper are fraud activities (such as physical theft) that leave no traces in the ERP/AIS system (for example in the form of postings or log files).

The occurrence of fraud is often explained with the help of the fraud triangle by Donald R. Cressey [25]. The fraud triangle comprises three generally accepted factors: pressures and incentives, opportunities, and attitudes and rationalizations (integrity). According to this model, people act fraudulently when all three factors have been fulfilled. Incentive is the perceived pressure that “drives” a person to commit fraud (dissatisfaction with the job). Rationalization is the attitude towards fraud and respect for rules and following those rules (internal justification, attitudes) [26]. An opportunity includes the danger of being caught. As Srivastava et al. emphasize, the relationship between the three factors has a special significance [27]. The risk for fraud increases exponentially when there is an increase in the connection between incentives, opportunities and rationalizations.

During a classic fraud audit, the analysis mainly focuses on data from the information system. It checks for conspicuousness in business transactions using, for example, Benford's law [28], limit value controls, special receipts and unusual posting times. There are various statistical and mathematical methods that help distinguish between usual and unusual transactions. In this way, analytical procedures can be used to find deviations between forecast and actual business values [29]. Data mining techniques can be used to analyze larger amounts of data [30]. Jans et al. use a descriptive data mining strategy with a multivariate latent class clustering algorithm to procurement data to assess the risk of internal fraud [17].

4. The concept of continuous auditing

Internal audits are performed on a regular basis and more and more often, they include the IT infrastructure. In order to be able to process such large amounts of data in a timely manner, they require “a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors’ reports issued simultaneously with, or a short period after, the occurrence of events underlying the subject matter” [31]. Essentially a continuous audit is a timely or real-time audit. This is accompanied by the extensive automation of the proper audit and evaluation steps. [32]

The continuous auditing method can be roughly split into two architecture methods. In the first method, the audit technique is integrated directly into the information system to be looked at as a software module (embedded audit module, or EAM) [33] [34]. In the second method, the audit technique is installed and operated separate from the information system. For the actual audit, a monitoring control layer (MCL) creates a connection to the monitored information system or the database [35]. In the recent past, other methods were developed to complement the two most often used ones, EAM and MCL, such as the interceptor mechanism [36], ghosting approach [18] or data-oriented online auditing (DOOA) [37]. All approaches have their pros and cons, which can lead to problems depending on the existing system landscape. In heterogeneous system landscapes, the use of EAM, which requires a highly system-specific level of implementation, can be quite time consuming and complicated. Implementation requires a high level of technical understanding, exact knowledge of the
system and can have a negative effect on system performance [18]. The MCL method, on the other hand, only has to be adapted to system-specific data interfaces. This process usually requires much less technical effort and the system is not approached invasively, meaning performance is not affected.

We aim to obtain fraud audit reports in real time. Therefore, we use the MCL method, by which we obtain data from various source systems via interfaces. This includes the required standardization of data collections. For example, free form text input fields should be avoided as source, because too much manual cleanup effort will be required [32]. This is done with the aim to automate the evaluation process as much as possible and to minimize or avoid manual intervention.

5. Differentiation among audit data

Because fraud takes place using both known and unknown patterns, it is necessary to analyze the entire data pool as part of an investigation. Differentiating among the data before the analysis supports a risk-oriented approach. Especially during a continuous audit, the focus of the audit can be determined and the circumstances that appear to be the most relevant can be prioritized.

We seek to deliver a practical argument for the consideration of human behavior. Human behavior should be included in an audit, because it prioritizes the data set and can be considered risk-oriented.

Because fraud takes place using both known and unknown patterns, it is necessary to analyze the entire data pool as part of an investigation. Differentiating among the data before the analysis supports a risk-oriented approach. Especially during a continuous audit, the focus of the audit can be determined and the circumstances that appear to be the most relevant can be prioritized.

We seek to deliver a practical argument for the consideration of human behavior. Human behavior should be included in an audit, because it prioritizes the data set and can be considered risk-oriented.

From a fraud perspective, transactions can be classified into usual and unusual (Figure 1). A transaction can be classified as unusual, for example, if it occurs during holidays or is posted with amounts slight below the release limit. During a fraud audit, predefined and known fraud signatures are applied to limit the amount of unusual transactions (section 3). By taking suspicious and non-suspicious human behavior into account, it is possible to uncover transactions that are part of a pattern (unknown fraud signature) that is not yet known and that would have been left undiscovered if using normal means. Critical or suspicious behavior can be assumed, for example, if an employee tries to circumvent permissions and system restrictions or if he was logged in at unusual times (e.g. at night or during holidays).

Figure 1 shows that the amount of data that should be prioritized increases for case 2 when taking suspicious behavior of employees into account. It also enables sophisticated investigation into the unusual transactions because they are classified into case 3 and case 4. We assume that the majority of transactions by employees with non-suspicious behavior are unremarkable (case 1). The usual transactions with suspicious behavior (case 2) and the unusual transactions with non-suspicious behavior (case 3) follow. The lowest, but most critical part consists of unusual transactions and suspicious employee behavior (case 4).

<table>
<thead>
<tr>
<th>Case</th>
<th>Transaction</th>
<th>Employee behavior</th>
<th>Potential threat classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Usual</td>
<td>Non-suspicious</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>Usual</td>
<td>Suspicious</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>Unusual</td>
<td>Non-suspicious</td>
<td>Medium</td>
</tr>
<tr>
<td>4</td>
<td>Unusual</td>
<td>Suspicious</td>
<td>High</td>
</tr>
</tbody>
</table>

The data parts shown in Figure 1 are prioritized in Table 1 using the potential threat classification (PTC) low to high, in which case 1 receives the lowest level priority and case 4 the highest. Classification enables us to perform a risk-oriented differentiated analysis.

6. Introducing the generic architectural model

We designed a continuous auditing architecture that makes sufficient allowance for the fraud triangle factors (section 3). In this way, in addition to the classic quantitative analysis of business transactions that are already being applied as part of the fraud detection audit, the human factor is extensively integrated into the audit as a qualitative component. Layer A I-V of Figure 2 reflects the classic procedure of a continuous auditing application. This approach
includes extraction of audit data from the source systems using the MCL technique, processing using the predefined risk characteristics and then visualization of the results. Within the context of the fraud triangle, the opportunities factor hereby is taken into account.

The inclusion of the human factor is focused on the manifestation of various behavior patterns. Behavior patterns can be derived from the analysis of user-related data from one or more information systems. These are derived using the individual factors of the fraud triangle. The information systems selected in Layer B-D usually belong to the business infrastructure of every organization. The configuration and availability of this system offers the advantage that they enable us to draw conclusions about unusual and potentially fraudulent users across the organization. Layer B outlines an analysis based on the event logs of the AIS/ERP. Both a deviation analysis between actual and reference processes [5] and determining the social networks are possible [38]. Analogous to that, in layer C, the network traffic is analyzed. A permanent network behavior analysis (NBA) is performed to find deviations from the normal behavior of an employee in the network. All this considers the opportunities factor. For example, otherwise unauthorized access to protected and sensitive areas (e.g. HR) remains undiscovered. In layer D, text mining is performed on all organizational e-mail accounts to evaluate the basic mood of employees. Holton remarks that “automated ways to find e-mail fraud indicators are very promising for reducing fraud losses.” [10] In this way, the fraud triangle is taken into account because “Organizations' abundant e-mail archives provide a path for detecting fraud incentives and potential for rationalization.” [10] The mood of e-mail writers can be determined by analyzing word choice and frequency.

The optional layer E outlines the connection of plug-ins. Plug-ins can help to take the three fraud

<table>
<thead>
<tr>
<th>Layer</th>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Extract raw data from source</td>
<td>Analyze raw data</td>
<td>Prepare audit data for aggregation</td>
<td>Aggregate data</td>
<td>Display fraud database</td>
</tr>
<tr>
<td>B</td>
<td>AIS / ERP</td>
<td>Process analysis</td>
<td>Process activities</td>
<td>Fraud database</td>
<td>Dashboard</td>
</tr>
<tr>
<td>C</td>
<td>Network traffic</td>
<td>Network behavior analysis</td>
<td>User (un)usual behavior</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>User mails</td>
<td>Email text mining</td>
<td>User mood</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>Plug-in e.g. SNS</td>
<td>Analysis</td>
<td>Audit data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 2. Generic architectural model
triangle factors into account in as much detail as possible, making use of additional information. This is conceivable for the factors incentives and rationalizations, in connection with social networking sites (SNS), instant messenger logs or extensive psychological predisposition tests [39].

The individual results of the analyses from layer A-E are summarized in a fraud database (layer IV) on user level (e.g. using a unique user ID). Finally, the results are prepared for auditors and high/level management using a dashboard (layer V). The dashboard enables individual analysis of results via various views. It provides both an overview of hazardous transactions in connection with behavior analysis of the person who made them and access to detailed data sets per drill down. Critical data sets are specially highlighted, considering the partial amounts shown in Figure 1. Prioritizing is done using Table 1, where partial amount 1 has the lowest priority level and partial amount 4 the highest. Case-related best practices are suggested for further examination.

The time it takes to realize the generic architectural model depends on the individual components. A data and process analysis can be implemented much more quickly than components that require a learning phase, such as network components or e-mail text mining.

7. Concept of a prototype

We describe here the concept of a prototype based on the generic architectural model from section 6 with an available SAP ERP 6.0 multitenant test system as a source for transactional data. Currently, the prototype is at an experimental state. The components described below are not yet fully integrated, manual steps are still necessary.

Figure 3 illustrates the generic architectural model introduced in section 6, in which a concept for practical implementation is introduced using freely available or open source tools where useful. The AIS/ERP shown in layer A, Layer I is an SAP ERP 6.0 system. The data required for the fraud analysis was extracted from this system (e.g. the tables BKPF, BSEG, USR02). In the next layer, the data written to a database is analyzed using Picalo [40]. Picalo is a data analysis software that, analogous to ACL [41] and IDEA [42] focuses on fraud detection. It is used for both simple and more complex script-based analyses. Special analyses, such as Benford or Gap analyses are part of the standard functions. The results of the Picalo analysis are supplemented with results from other analyses (B-D).

Extracted process logs from the same SAP ERP 6.0 as used in layer A are used as input in layer B. To
compare actual and reference processes, we import the logs for analysis into ProM using an intermediate database. ProM is a platform independent process mining tool that supports plug-ins for various analyzing or mining functions [43] [44].

A further component of our model is the network component shown in layer C. The network data communication of a Cisco router is exported and can be called up by the software FlowMatrix [45] in the NetFlow format. NetFlow is a standardized network protocol for traffic monitoring and includes information on data traffic [46]. Behavioral changes in employees are determined with the help of network behavior analysis. An initial learning period is required before deviating behavioral patterns, assuming IP addresses and the associated usernames are available. The usual observation period takes 7-14 days.

A Microsoft Exchange Mail Server is used as the data basis for layer D. A conversion of the proprietary Microsoft Exchange Mailbox Format into plain text e-mail format mbx is required in order to be able to perform text mining on the e-mails. Text mining is done using general architecture for text engineering (GATE) [47]. The GATE components are controlled using Meandre [48], which enables automated text mining in the form of a workflow. The result classifies the general mood of the employees, for example, as disgruntled or non-disgruntled. This procedure was already described and successfully evaluated by Holton [10].

The results of layer B-D of Layer III are summarized in a user fraud ranking database. A potential threat classification (PTC) is then determined from the individual results, taking the weighting factors into account. For the introductory phase, in our model we used an equal weight distribution. Later, each organization can adjust the weighting of factors individually after the evaluation phase is over, and using the empirical values from that phase.

In order to keep the model practice-oriented and comprehensible, we use the following calculation for the aggregation (PTC) of the individual values:

$$PTC = x_1 B + x_2 C + x_3 D$$

where $PTC =$ potential threat classification; $x_1 = x_2 = x_3 = 1$ – weighting factors; B, C, D element of $\mathbb{N} \{0, 1\}$ – classification, with 0 – non suspicious; 1 – suspicious.

The classification described in section 5 was taken into account when we visualized the dashboard. The overall assessment was mapped using traffic lights. The cases (case 1) that were classified in Table 1 as low PTC (transaction usual, employee behavior nonsuspicious) got green light. A yellow light is given when the PTC is not equal to zero or the transactions are considered unusual (medium: case 2 and 3). The highest warning level (high) is output for case 4. The traffic light is red when the transactions are unusual and the PTC was not equal to zero.

The results are visualized using SAP Crystal Dashboard Design [49]. This front end offers the auditor and/or high-level management the information required for further analysis. The various predefined views can be controlled using a defined authorization concept by target group.

8. Discussion

Many of the concerns discussed in the literature refer to the analysis of personal data and the possible breach of personal privacy of employees as well as ethical concerns [10] [20] [50] [51] [52]. Here the legal and data protection regulations of the particular country must be taken into account [53]. It is absolutely necessary to perform an organization specific check. An example of this is text mining of e-mails, as discussed in section 7. For reasons of privacy, auditors generally do not have access to the e-mails being analyzed. Only in the case of a confirmed suspicion when further investigations have been launched this type of access is permitted. E-mails are important pieces of internal business data for which there is an obligation toward archiving and documentation. In this case, employees only have limited rights to privacy [50].

It is important to get a balance between privacy and monitoring. While monitoring can damage the trust relationship within organization and negative affect employee productivity and cooperativeness, its absence can result in insider actuation [52]. Regarding to Greitzer et al. [51] the maximum tolerable level of monitoring depends on organization and country-specific rules and should be determined considering advises of corporate legal counsel.

Another point of discussion is the analysis of human behavior and dealing with the results. It must be noted that unusual behavior is not synonymous with the intention of actually committing fraud or with having committed fraud [10]. Risk indicators can be derived from behavior that raises suspicion of fraud. These indicators must be weighed against principles of professional judgment and can be used as a starting point for further intensive checks. The costs of not discovering the fraud (false negatives) exceed the expected additional expenditure of pursuing false positives. “With total accuracy clearly out of reach, false positives are preferred to false negatives...” [10].

The exact measure of prevention or combating fraud can be selected specific to the organization. With
regard to prevention, awareness-building measures have proven to be helpful among employees [54].

Beyond that, the combination of the PTC provides another point of discussion that requires separate evaluation. In section 7, we determined that the selection of weighting factors must be done by each organization. As part of a future case study, we need to check whether modifying the PTC calculation can provide a more precise risk classification of employees. This can, for example, be done based on work from Srivastava et al. [27] and Turner et al. [55], who have already done mathematical work on the possible connections between fraud triangle factors.

9. Conclusions and outlook

We introduce a generic architectural model that has sufficient allowance for the fraud triangle factors. In this way, in addition to the classic quantitative analysis of business transactions that are already being applied as part of the fraud detection audit, the human factor is extensively integrated into the audit as a qualitative component. This provides added value because the transactions examined by the auditor can be better differentiated and prioritized. By taking suspicious and non-suspicious human behavior into account, it is possible to uncover transactions that are part of a pattern that is not yet known and that would have been left undiscovered using normal means. The inclusion of the human factor is focused on the manifestation of various behavior patterns. These behavior patterns can be found in user data. E-mails are examined using text mining, a network behavior analysis is performed on network traffic and the ERP/AIS process logs are analyzed. The generic architectural model can be expanded in a modular way by adding plug-ins. The proposed architecture is implemented using a prototype and is applied exemplary to an SAP ERP system. We suggest a selection of established tools for implementation.

Legal regulations and ethical concerns may represent the largest obstacle to the practical implementation of the prototype. Beforehand, it is very important to clarify how the respective legal regulations permit unlimited use in an organizational context. The modular structure of the prototype enables step-by-step implementation of the permitted components. It is also necessary that the auditors have the required expertise, and they are well versed in both fraud and the technical operation of the individual components (e.g. scripting). The approach developed in this paper provides support and can relieve the auditor, but it does not replace the required basic experience and knowledge. Because it is important to remember that the indication of suspicious behavior concerning fraud does not mean that fraud has taken place or that there was intent to commit fraud. The generic architectural model presented is part of a further and more intense research effort.

Our future work will concentrate on evaluating the introduced prototype using case study research. The interrelation between risk indicators, weighting factors, and the PTC needs to be looked at in more detail. Another goal is the implementation as a complete automatic continuous auditing tool for real-time assessments. To this end, the degree of automation of the tools that are linked to one another must be increased and manual intervention in the analysis process must be reduced to an absolute minimum. Another interesting aspect of plug-ins is connecting to social networking sites. In this way, ideally, additional information on the social networks of employees can be extracted, and this information can be useful for fraud analysis. It is conceivable that personality profiles be investigated scientifically in order to better connect the behavior respectively human factor and to make even more precise risk estimations. Conceivable is also to examine whether investigating personality profiles can lead to more precise predictions during e-mail text mining. Another imaginable approach is using neural networks. These are especially known for their ability to recognize patterns in data. The connections found in this way can be used successfully for prognoses. Detection and prognosis of employee behavior or analysis of business transactions could be promising new areas of application.

10. References


