Routledge
Taylor & Francis Group

TECHNOLOGICAL AND ECONOMIC DEVELOPMENT OF ECONOMY
ISSN 2029-4913 print/ISSN 2029-4921 online

2011 Volume 17(3): 535–561
doi:10.3846/20294913.2011.602440

# METHOD FOR SELECTION OF MOTOR INSURANCE FRAUD MANAGEMENT SYSTEM COMPONENTS BASED ON BUSINESS PERFORMANCE

**Štefan Furlan[1], Olegas Vasilecas[2], Marko Bajec[3]**

*[1, 3]Faculty of Computer and Information Sciences, University of Ljubljana, Tržašlka cesta 25, Ljubljana, Slovenia*
*[1]Optilab, Zupančičeva 8, 5270 Ajdovščina, Slovenia*
*[2]Vilnius Gediminas Technical University, Saulėtekio al. 11, LT-10223 Vilnius, Lithuania*
*E-mails: [1]stefan.furlan@fri.uni-lj.si (corresponding author); [2]olegas.vasilecas@vgtu.lt; [3]marko.bajec@fri.uni-lj.si*

*Reveived 27 April 2011; accepted 22 May 2011*

**Abstract.** Fraud in motor insurance is assessed to incur annual losses in the range of 100 billion dollars. While much research exists in the fraud management field, majority only deals with partial problems and presupposes the independence of specific fraud management activities. Researches on components of fraud management system are rarely explicitly related to business performance improvements. These results in a common problem, which can be observed on the practitioners' side: only small amount of companies can objectively assess which of the many fraud management system components proposed by researchers and vendors will help to solve their problems in fraud management. The method proposed in this paper can be used as a strategic tool for improvement of fraud management process in motor insurance companies. The method is designed to be used for a selection of fraud management system components, and is based on business performance. The input for the method is a set of key performance indicators that an insurance companies wish to improve. The result is a set of activities, which should be improved, and a set of fraud management system components that should be used to improve these activities. The paper presents and explains the method and its components. The method components have been developed based on the data received from Slovenian motor insurance companies and method is evaluated in three case studies.

**Keywords:** fraud management, fraud management system, fraud management system development, business performance, key performance indicators, motor insurance.

**Reference** to this paper should be made as follows: Furlan, Š.; Vasilecas, O.; Bajec, M. 2011. Method for selection of motor insurance fraud management system components based on business performance, *Technological and Economic Development of Economy* 17(3): 535–561.

**JEL Classification:** C88, C61, G22.

## 1. Introduction

Fraud in motor insurance is a recognized problem and is assessed to incur losses in the range of 100 billion dollars annually[1,2]. At the Insurance Fraud conference 2010[3] in London, several facts were uncovered by practitioners. Zurich Financial Services[4] amongst others reported an increase of fraud in all lines of insurance in 2009 due to bad global economic situation. Association of British Insurers[5] assessed the cost of insurance fraud in Britain in 2009 to 2.63 billion £, which is a 26% increase in two years.

Computer technology was recognized as one of the efficient techniques to tackle insurance fraud, see e.g. (Derrig 2002). We define fraud management system as all software and information system components, used to support all fraud management activities, i.e. fraud detection, prioritization, investigation, mitigation, redress, sanctioning, deterrence, prevention, activities related to continuous system improvement and activities related to monitoring. Fraud management system is composed of many components, out of which fraud performance components are the most widely known and publicized.

The premise upon which we base our research is that *introduction of a fraud management system component is an action aimed at improving business performance*, i.e. reducing cost of fraud.

It has been shown that in order to be able to improve the performance, one must first know how to measure it. The detection or practice in fraud management field have so far not provided a concise system of metrics or key detection indicators (KPI) to measure fraud management business performance. There is, however, some research, see e.g. (Phua *et al.* 1998; Bonchi *et al.* 1999; Viaene *et al.* 2007), that measures the results of the research against some business relevant KPI. Research results are mainly only compared to research relevant metrics e.g. classification accuracy, AUROC etc. Such approach is problematic from two perspectives. Firstly, in most cases, research results are incomparable even for different proposed solutions for the same issue, e.g. fraud detection component. Secondly, practitioners have no clear idea as to how implementation of a proposed solution would affect their business performance.

Research provides a lot of different solutions for fraud management system components, se e.g. (Artis *et al.* 1999; Brockett *et al.* 2002; Dionne *et al.* 2009). All research, however, provides only partial solutions, addressing individual components, and not fraud management system as a whole. Fraud management activities are not independent. For example, being able to detect all fraudulent cases will not yield any results if the investigation and redress activities are unsuccessful. In practice, if a fraud management component as a partial solution is implemented, it may only affect business performance partially or even decrease overall business performance, if component was not properly selected.

There is a clear need in research and practice to provide a link between fraud management system components and their effect on fraud management business performance. We propose an actionable method that can be used in such a manner. With our method, companies

[1] Insurance Fraud Bureau, <http://www.insurancefraudbureau.org>.
[2] National Insurance Crime Bureau, <https://www.nicb.org>.
[3] Insurance Fraud 2010, <http://marketforce.eu.com/Conferences/claimsfraud10/>.
[4] Zurich Financial Services, <http://www.zurich.com>.
[5] Association of British Insurers, <http://www.abi.org.uk>.

can first measure fraud management business performance. When companies are deciding, which business performance is in need of improvement, our method enables them to learn which activities need improvement and which fraud management system component can support these activities.

The method presented in this paper is limited to motor line of insurance and to reactive part of fraud management, which covers the activities of reacting to insurance claims, i.e. fraud detection, prioritization, investigation, redress, mitigation and sanctioning.

The rest of the paper is structured as follows: in the second section research method is introduced, then related work. Following is the introduction of our method in general, all method components and the method use case. Fifth section presents a case study to support our research. The paper concludes with discussion and acknowledgments.

**Research method**

The research was conducted in three phases, as depicted in Fig. 1: method construction, method evaluation and results interpretation. Different research methods were utilized, namely literature review, expert interview and case study. The research process and methods used in individual phases are depicted in the bottom figure. Literature review is presented in section 2 of the paper, different types of expert interviews are presented in this section and the method itself is presented in section 3. Case study, method evaluation and interpretation of results are presented in sections 4 and 5.

The research began with extensive literature review. All relevant literature was considered, both in the broad research area and the narrow research area. The first version of the three method components is based literature: KPIs, activities and FMS components. In the first series of expert interviews, the goal was to discuss, evaluate and extend the three method components obtained from the literature review.

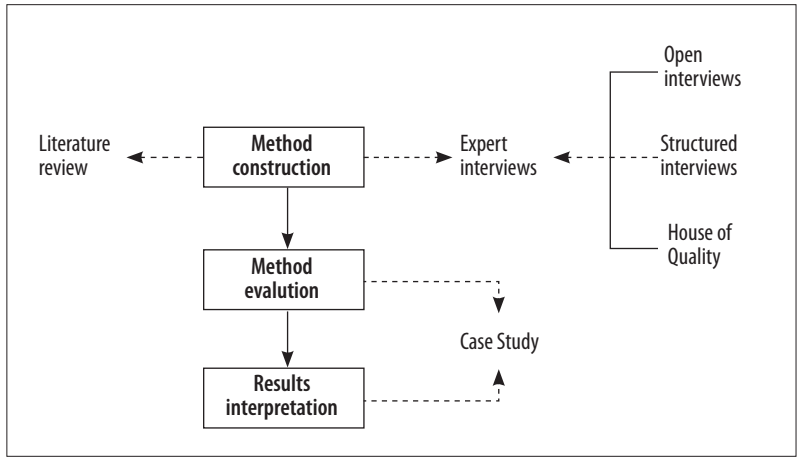


**Fig. 1.** Research method, boxes depict research phases and underlined text denotes research methods used in corresponding stages

Domain experts were consulted with the help of expert interviews. Domain experts were people responsible for fraud management in six Slovene motor insurance companies, ranging in premiums from roughly 50 million € to 750 million €, and in special fraud investigation units sized from one-man-band to more than 35 people. The conducted case study observed three implementations of three different FMS components in these insurance companies.

Structured interviews were used to construct a KPI/activity matrix. Each of the domain experts was asked to provide KPIs for their organization and to provide an assessment of the maturity level for each process. For the maturity assessment CMMI[6] was utilized, which presupposes the following maturity scale: initial, managed, defined, qualitatively managed and optimizing process. According to the maturity level of each activity domain, experts assigned a grade from 1 to 5, with 5 being the best – optimizing process. Correlation between activities and KPIs was assessed using standard Pearson's chi-square statistic. The peak correlation was observed between KPI "Average investigated claim value" and activity "Prioritization" (see Figure 4). The later does not indicate statistically significant correlation, as one would expect due to low number of examples. Moreover, considering the chi-square distribution, for the above correlation to be significant one would need data from at least e.g. 40 insurance companies, which is extremely difficult. Insurance companies are very reluctant to share sensitive internal business performance information and it took over one year to convince all insurance companies in Slovene market to cooperate and to collect all the information needed here. The research continued with the correlations as-is (the 10% most correlated pairs were treated as "very correlated" and the following 25% as "mildly correlated"), as it was planned to test the final method on three independent case studies, method sufficient to confirm the hypothesis.

Structured interviews based on a House of Quality were used to construct the activity/FMS component matrix. House of Quality (Hauser, Clausing 1988) is part of quality function deployment method, which has been used in similar tasks before (Matook, Indulska 2009). House of Quality is a method and artefact used to correlate company needs in certain activities and product characteristics. In our research, we used House of Quality to correlate insurance company needs in activities to FMS components. First the process activities were split down into their individual goals and each of the experts was asked to apply each goal an overall importance score, ranging from 1 to 10, 1 meaning not important in fraud management context and 10 meaning most important. Averaged expert scores are presented in a correlation matrix (Fig. 5) in a column "Importance (average expert score)".

Late the FMS components were introduced to the experts and they were asked to answer the questions "How much can component X help in achieving process goal Y?" for each activity goal and each FMS component. Possible answers were as follows: "does not help", "mild", "moderate", and "very". The answers were applied with scores of 0, 1, 3, and 9, respectively. Using 1, 3, and 9 scores is strongly advised when using House of Quality (Matook, Indulska 2009). At the end the scores were averaged to construct an activity/FMS component matrix.

The method, i.e. all method components: KPIs, KPI/activity matrix, activities, activity/FMS component matrix and FMS components , was thus constructed from literature review and three series of expert interviews.

The method was evaluated in three case studies. The method was applied in different companies, implementing three different FMS components. For each of the companies, first,

[6] Capability Maturity Model Integration, <http://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration>.

potential improvements were identified. Company selected KPI that was lacking the most compared to industry average. Then, the method was used to identify the FMS component that would affect the performance in that particular area. One year after the implementation the old performance was compared against the predicted increase and an actual increase of performance.

## 2. Related work

The broad research area is fraud management in general and narrow research area is fraud management in motor insurance. The most active domains in the broader research area are telecommunications fraud, insurance fraud, healthcare fraud, corporate fraud, internet click fraud, money laundering and credit card fraud. In literature, topics related to fraud management can be found under different terms, such as fraud detection, fraud prevention, techniques to tackle fraud, fraud classification, recognizing fraud, fraud investigation, fraud deterrence, abuse detection/prevention or just fraud.

Table 1 provides an overview of the most relevant literature that is presented later in this chapter. Literature is classified according to the fraud management process activity and to the level of abstraction.

Methods for automatic fraud detection range from statistical methods (Artís *et al.* 2002; Bermudez *et al.* 2007), expert systems (Major, Riedinger 2002; Viaene *et al.* 2004), data mining (Viaene *et al.* 2005; Peng *et al.* 2006), visual and analytical methods (Tie 2010; Chang *et al.* 2007; Sokol *et al.* 2001) and others. There are, however, also manual ways to detect fraud, such as report from claims adjustors or appraisers, via hotlines etc. One method does not fit all types of fraud, which is why insurance companies must employ and successfully combine different methods (Silverstone, Davia 2005). As the environment constantly changes and fraudsters change their tactics (Bolton, Hand 2002; Cahill *et al.* 2002; Fawcett, Provost 1997; Tuyls 2000; Xing, Girolami 2007), fraud detection and prioritization must be adaptive (Sternberg, Reynolds 1997).

Statistics has been applied to fraud management in broad research area (Bolton, Hand 2002; Aggarwald, Yu 2005; Barbará *et al.* 2006). Statistical methods are used to detect deviant behaviour, and are especially useful in domains with no labelled data. The most common statistical approaches applied to fraud detection are outlier detection (Aggarwald, Yu 2005) and statistical profiling. Profiling is a common technique to detect fraud, used mainly in telecommunications (Fawcett, Provost 1999; Cahill *et al.* 2002; Boukerche *et al.* 2004; Abidogun 2005; Xing, Girolami 2007), but also in banking (Chang *et al.* 2007) and health insurance (He *et al.* 1997; Major, Riedinger 2002). In telecommunications profiling is used to detect suspicious calling patterns, sudden fraudulent changes in calling patterns and to differentiate legitimate changes in behaviour (Xing, Girolami 2007) from the fraudulent ones. Profiling produces good results in domains with a lot of business events, e.g. telephone calls, bank transactions and medical services. Relative to the broad research area, there is not much use of statistics in fraud management for motor insurance. Profiling for example has not yet been applied to motor insurance, where we see a great potential, especially related to insurance agents, claims adjusters, appraisers and other insurance employees to detect internal fraud, and also in relation to external entities with large quantities of business events, such as auto repair shops, lawyers and medical practitioners.

Expert systems enable encoding human expert knowledge into a computer system (Gudas 2009) and utilizing that knowledge (Kalibatiene, Vasilecas 2010; Lavbič *et al.* 2010) to solve expert level problems. The knowledge is encoded in a so called knowledge base in form of easy-to-understand rules. In fraud detection literature, these rules are also referred to as red-flags, indicators, fraud controls and expert rules (Furlan, Bajec 2009; Major, Riedinger 2002; Viaene *et al.* 2004; Garner, Chen 1994; Sternberg, Reynolds 1997; Bordoni, Facchinetti 2001; Curet *et al.* 1996; Sun, Finnie 2004). Expert systems are seldom used in fraud detection for their good explain capability, which is very valuable in the investigation phase, when fraud investigators need to understand the situation and communicate with fraudsters (Viaene *et al.* 2002).

There are two specifics of data mining that must be taken into account when building fraud detection models. (1) The general binary models need to be adaptive, as nature of fraud is very dynamic, since investigators' actions instantly trigger reaction from fraudsters, who are constantly adapting their practices to stay below the fraud detection radars. (2) Most methods need a good labelled learning set, which is not a realistic demand. A bad learning set, on the other hand, yields a high probability of omission error (Artis *et al.* 1999, 2002; Caron, Dionne 1999). But here we will focus on supervised methods. Classification is a data mining approach, which assigns objects (persons, claims, events etc.) based on their features with one of predefined classes. Fraud detection is the most common fraud management activity to utilize classification techniques. Binary fraud/non-fraud classifiers are the most common, although classification can also be applied to detect more specific types of fraud, e.g. fraudulent whiplash (Gudmundsson *et al.* 2010). In the fraud management research related literature one can find different classification algorithms, ranging from simple ones, such as Naïve Bayes, k-Nearest Neighbors and Decision Trees, to the more complex ones, such as Neural Networks and Support Vector Machines (Gudmundsson *et al.* 2010; Viaene *et al.* 2002, 2005; Brockett *et al.* 2002). A comprehensive analysis and comparison of classification algorithms for fraud detection has been conducted by Viaene (2002). He showed that no algorithm significantly over performed in all scenarios, and that even very simple algorithms yield good overall results. The lack of labelled data is a barrier to test more data mining methods (Bolton, Hand 2002; Phua *et al.* 2005). In the telecommunications fraud detection, there had been several attempts to automatically generate data (Lundin *et al.* 2002; Barse *et al.* 2003), but the results lacked the authenticity needed for quality machine learning. It is also well-known that omission error is very common in motor insurance fraud detection datasets (Artis *et al.* 1999, 2002; Caron, Dionne 1999). Many authors pointed out (Tuyls 2000; Phua *et al.* 2005; Cahill *et al.* 2002, Viaene *et al.* 2002) that simple classification accuracy or AUC (Viaene *et al.* 2002) is not an appropriate evaluation method because of skewed data and because of the different values of claims. Cost-based methods are noted as the most suitable for this domain (Viaene *et al.* 2007; Stolfo *et al.* 2000). An overview of on-line-accessible English publications on using data mining methods for financial fraud detection, including motor insurance fraud, can be found in (Ngai *et al.* 2010). We believe that there is a great potential in constructing specialized classifiers to detect specific types of fraud, such as whiplash (Gudmundsson *et al.* 2010) and other frauds related to currently challenging types of fraud, such as fake or exaggerated personal injuries and claims farming.

The investigation resources are always scarce. From all detected suspicious claims, insurance company needs to select the most perspective ones for the investigation (Bond, Crocker 1997; Tennyson, Salsas-Forn 2002). The task of assigning a relative importance value to the claim is referred to as ranking or prioritization. A task can be a part of data mining model, when using regression or statistical models (Brockett *et al.* 2002; Viaene *et al.* 2002); or a score can be assigned later (Dionne *et al.* 2009). In theory, there are three types of values that can be used for ranking. First is probability of fraud (Brockett *et al.* 2002; Bolton, Hand 2002; Phua *et al.* 2005; Viaene *et al.* 2002). The majority of authors (Viaene *et al.* 2007; Dionne *et al.* 2009) advocate probabilistic approach to determine suspiciousness, although some more complex approaches can also be found in literature (Brockett *et al.* 2002). The second value is price (Dionne *et al.* 2009), which must include both claim value (Viaene *et al.* 2007; Bond, Crocker 1997) and predicted investigation costs (Viaene *et al.* 2007). The higher the difference between case value and assumed investigation costs, the more perspective is the case. It is not possible to know the exact cost of investigation and the final claimed amount beforehand. The research showed, however, that assuming average investigation costs and assessed claim value yields good results (Viaene *et al.* 2007). The third value is the ability to redress (Furlan, Bajec 2009). There is a research combining cost and probability of fraud (Vieane *et al.* 2007), but we argue that the ultimate score should comprise of all three factors. One major issue related to prioritization remains unaddressed so far. Many insurance companies use different methods to detect different types of fraud, but the research has not yet proposed the joint ranking algorithm to consolidate results from different methods.

There are many common investigation techniques that are usually employed, such as enquiries to industry bureaus, rating agencies or other available information providers, site investigations, surveillances, independent medical examinations, medical audits, sworn statements, recorded statements, special investigations, wage verifications etc. (Derrig *et al.* 1994; Radcliffe 1995; Weisberg, Derrig 1998; Tennyson, Salsas-Forn 2002) Insurance companies often make use of different software components such as visual and analytical tools to visualize and visually investigate data (Sokol *et al.* 2001; Chang *et al.* 2007), and other computer techniques such as automatic text analysis (Popowich 2005), and lie detection in recorded statements with the use of voice stress analysis (Hollien *et al.* 1987). If using automated fraud detection, it has been shown (Viaene *et al.* 2004) that methods, that yield better explanation capability produce better results in investigation as they provide explanation of suspicious circumstances, rather than providing merely a vague suspicion score. An expert system is an example of such a technique (Garner, Chen 1994; Bordoni, Facchinetti 2001; Major, Riedinger 2002; Viaene *et al.* 2004). Neural networks-based methods on the other hand, however, have been often criticized to lack such explanation capability (Viaene *et al.* 2002). Dynamic nature of fraud makes it harder to detect it with static fraud detection algorithms (Cox *et al.* 1997; Žagar 2008). On the other hand, the same issue can be solved very efficiently by providing the investigator with a visual overview of data, helping the investigator to interact with data, easily comprehend the situation, and consequently draw conclusions (Chang *et al.* 2007; Sokol *et al.* 2001; Žagar 2008). Visualization as a method for fraud investigation can be divided into two categories: general data visualization and fraud reports. The general visualization methods applied to fraud detection and investigation are different types of charts, such as bar charts (Chang *et al.* 2007; Sokol *et al.* 2001), pie charts (Sokol *et al.* 2001), and line charts (Chang

*et al.* 2007; Sokol *et al.* 2001). In literature, one can also find more sophisticated techniques, such as heat maps (Chang *et al.* 2007), networks (Cox *et al.* 1997; Žagar 2008; Chang *et al.* 2007; Tie 2010), parallel coordinates (Žagar 2008), sieve diagrams (Žagar 2008) etc. Additional visual enrichment can be achieved by introducing the temporal and/or geographical component (Žagar 2008; Chang *et al.* 2007). A comprehensive overview of visualization methods for fraud investigation in telecommunication are presented in (Žagar 2008). The difference between general visualization methods and fraud reports is in the generality. Whilst the earlier described visualization methods, can be used to observe any data in any particular domain, fraud reports (visual or textual) are used in a specific domain, with specific data to clearly illustrate a specific type of fraudulent activity. Hyperbolic and circular graphs are used in telecommunications to visualize network of fraudsters (Žagar 2008), in banking to discover fraudulent transactions (Chang *et al.* 2007) and for connecting fraudsters and other entities, such as people, cities and organizations, in money laundering (Tie 2010). Cox *et al.* (1997) presents a networks visualization to display international fraudulent activities related to telecommunication. Chang *et al.* (2007) introduced a complex visualization, comprised of a heat map, a line chart, a bar chart and a hyperbolic graph, to point out suspicious banking transactions. We see potential in applying visualization methods from broader domain to motor insurance fraud investigation. We also see great potential in introducing more fraud reports to motor fraud detection and investigation, especially in relation to visual detection and investigation of novel fraud types such as claims farming.

The goal of fraud redress and mitigation is to redress the money lost or withhold the payment for fraudulent claims. The goal of sanctioning is in both seeking redress and sanctions, but also deterring further fraudulent activities (Jou, Hebenton 2007; NHS 2001). The actions that insurance companies usually exercise range from: do nothing, send warning, suspension, dismissal, civil proceedings to recover the money, criminal proceedings resulting in a fine, criminal proceedings resulting in a prison sentence (NHS 2006a, 2007). Although fraud is one of basic criminal offences, fraudulent cases are usually not passed to the prosecution. In fact, our industry research has shown that only 3% of investigated cases are passed on to the prosecution, the majority of which as a counter action to fraudsters pressing civil charges against insurance companies for declining their indemnities. The procedures vary from country to country (NHS 2006b), but the main reason for the lack of sanctioning actions from the insurance side lies in ineffective and slow actions from police and prosecution side (Selinšek 2004). There is no research focused on software components that can be used to support redress, mitigation and sanctioning activities, although there are some widely used concepts that could have been applied to these activities. To name just one example, business process management systems (BPMS) could be utilized to streamline the investigation process, and criminal and civil proceedings. BPMS are generally used to streamline and provide information technology support to business processes. The added values of BPMS are reported to be: increased visibility and control of company's activities and bottlenecks, more efficient process execution and better division of duties and responsibilities (Ko 2009).

Data is the basis for all fraud management system components, therefore research puts a lot of attention to different data sources, different methods of data storing and different methods of data (pre)processing. It has been shown that shared industry databases (Radcliffe 1995), databases and data warehouses (Nguyen *et al.* 2005; Sokol *et al.* 2001), and extracting

information from unstructured data sources by employing natural language processing (Popowich 2005), can be beneficial to fraud detection performance. Radcliffe encouraged using common, industry-shared claims databases and checking every new claim against the complete history. To our knowledge there has been no research related to importance of other databases, such as policy databases, vehicle databases etc., related to motor insurance fraud detection. The novel technology of data warehouses can be used to store a multidimensional database that is especially fitted to support analytical activities. Data warehouses are often utilized to detect fraud in telecommunication (Mattison 2005; TMF 2006; Nguyen *et al.* 2005), usually to provide underlying data for profiling, data mining, visualization and fraud reports. The demand (Nguyen *et al.* 2005) to achieve near real time data warehousing in telecommunication is not applicable to motor insurance fraud management. Regarding the data pre-processing, a procedure of Extract-Transform-Load (ETL) is commonly used for data preparation and cleaning for storing in data warehouse, data mining or other automated intelligent computer task. ETL is a well-known process in data mining, as data preparation consumes 80% of all data mining time on average (Sokol *et al.* 2001). Fraud management in gambling (Jonas 2006) and health insurance (Sokol *et al.* 2001) is faced with the following ETL issues: incomplete data, anomalies in data, unexpected characters and identity matching. The last issue is referred to as entity resolution. Jonas (2006) describes identity matching and identity resolution approaches in tackling fraud in gambling. Natural language processing (NLP) is used to process information from unstructured data. A lot of information in motor insurance is not structured, and NLP techniques are employed to either (1) extract important information from unstructured data sources, or (2) to categorize text, e.g. lie/honest. Information extraction is a common NLP problem (Peng, McCallum 2006), the most important subproblem being entity recognition, i.e. recognizing the elementary parts of text, such as geographic names, personal names, companies, dates, numbers etc. (Poibeau, Kosseim 2001). In text categorization on the other hand, specific solutions were constructed, especially for fraud management. In detecting fraudulent transactions in banks, Chang (2007) employed detection of coexistence of words that should not be related. In health insurance text mining was used to classify health insurance claims (Popowich 2005) into different classes depending on the nature of treatment. The useful contribution to practitioners would be to address and provide best practices to the most common ETL problems. We also believe that data warehouses could be successfully utilized in tasks of visualization, profiling and data mining in motor insurance.

As seen from the research, presented here, some areas, e.g. fraud management system components for fraud detection, receive a lot of attention, others, e.g. fraud management system components for redress, mitigation and sanctioning, on the other hand have so far received no attention. However, the biggest issue in motor insurance fraud management is that fraud management process activities are treated as independent. There are very few papers, see e.g. (Derrig 2002), addressing more than one activity, and even this research is not addressing the complete fraud management process. On the other hand, there is also very few papers, see e.g. (Becker *et al.* 2005), addressing the same activity in the different level of abstraction. Fraud management system components are discussed independently of the activities they are aimed at to support, and only a few papers are discussing single fraud management system components, see e.g. (Viaene *et al.* 2007), with respect to the concrete goals of fraud management on the level of business performance (see Table 1).

**Table 1.** Relevant contributions to fraud management, organized according to fraud management activity and level of abstraction. Table presents relevant contributions, found in literature from motor insurance and other domains where seen as relevant

| | | Activities | | | |
|---|---|---|---|---|---|
| | | **Detection** | **Prioritization** | **Investigation** | **Redress, Mitigation & Sanctioning** |
| Level of abstraction | Business performance (goals, cost assessment, business performance improvement) | Cost of fraud (Becker *et al.* 2005)<br>Detectable fraud (Derrig 2002; Becker *et al.* 2005)<br>Fraud type classification (Stolfo *et al.* 2000; Derrig 2002) | Investigation costs (Viaene *et al.* 2007) | Fraud control costs (Becker *et al.* 2005) | |
| | Activity (methods of activity execution, tasks description) | Fraud indicators (Brockett *et al.* 2002; Becker *et al.* 2005)<br>Using computer technology (Derrig 2002)<br>Detection tactics (NHS 2001)<br>Fraud detection (Schiller 2006)<br>Data pre-processing (Phua *et al.* 1998; Bonchi *et al.* 1999) | Sorting (Derrig 2002)<br>Scoring (Derrig 2002; Dionne *et al.* 2009)<br>Costly state verification (Bond, Crocker 1997) | Special investigation unit (Derrig 2002)<br>Investigation tactics (Derrig *et al.* 1994; Weisberg, Derrig 1998; NHS 2001; Tennyson, Sallas-Forn 2002) | Prosecution and sanction (NHS 2001; Derrig 2002)<br>Redress (NHS 2001)<br>Classification of redress, mitigation and sanctioning activities (NHS 2007)<br>Current issues (Selinšek 2004; NHS 2006a)<br>Case studies (Stempel 2002) |
| | FMS components (components, techniques, algorithms, methods) | Data mining techniques (He *et al.* 1997; Artis *et al.* 2002; Brockett *et al.* 2002; Viaene *et al.* 2004; Xing, Girolami 2007)<br>Statistical models (Garner, Chen 1994; Bermudez *et al.* 2007)<br>Expert systems (Sternberg, Reynolds 1997; Bordoni, Facchinetti 2001; Major, Riedinger 2002)<br>Method classification (Ngai *et al.* 2010)<br>Method comparison (Viaene *et al.* 2002; Ngai *et al.* 2010) | Cost sensitive prioritization methods (Viaene *et al.* 2007)<br>RIDIT scoring (Brockett *et al.* 2002)<br>Costly state verification (Bond, Crocker 1997) | Fraud reports (Major, Riedinger 2002; Chang *et al.* 2007; Tie 2010)<br>Visualization techniques (Cox *et al.* 2007) | |

The goal of the paper is to introduce an actionable method that connects the complete fraud management process from the business performance level through process activities to fraud management system components. The method can be used in two ways, (1) to assess, which fraud management system components should be implemented to increase performance of a specific KPI, and (2) to predict what kind of effect an implementation of a specific fraud management system component on business performance will have.

## 3. The method

### 3.1. Method introduction

The method is based on the business process meta-model (Eriksson, Penker 2000). Business process meta-model defines the relations between the business concepts in an organizational environment.

As depicted in Fig. 2, business process meta-model introduces an organizational goal, which can be measured with one or more key performance indicators (KPI). Goals are

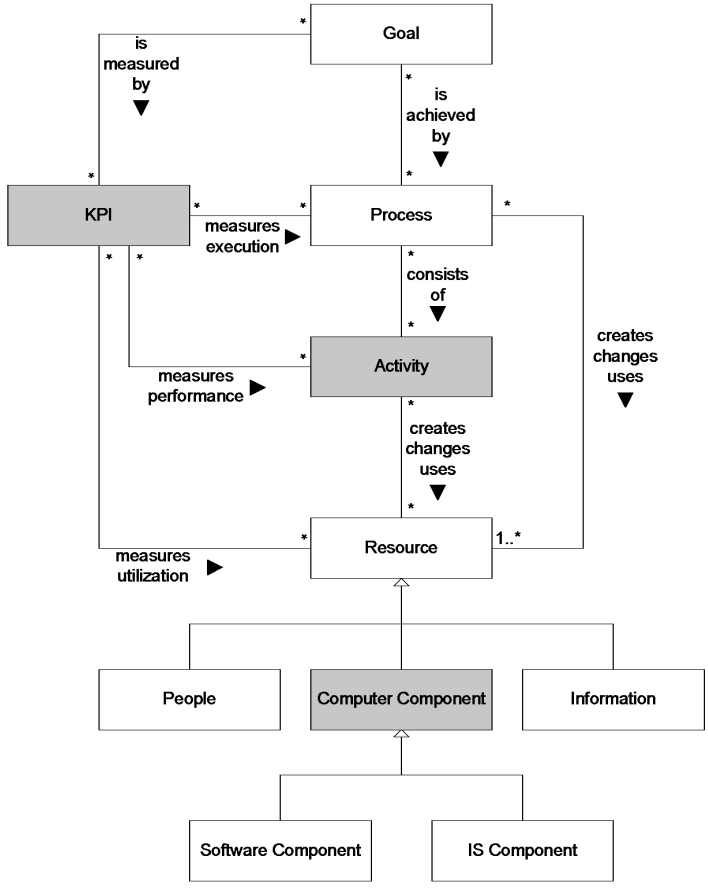


**Fig. 2.** Business process meta-model

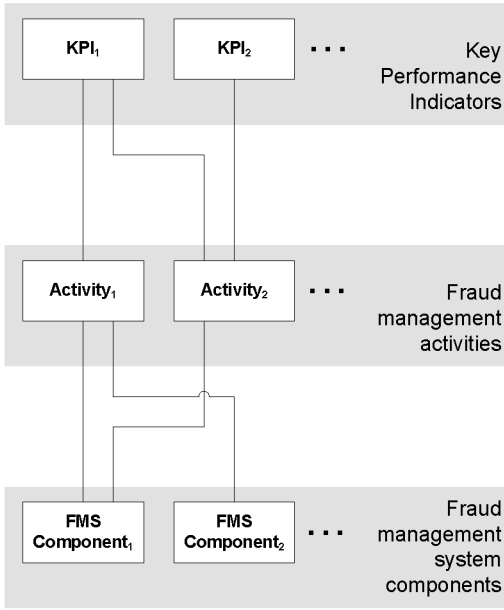


**Fig. 3.** Method model

achieved by executing processes and KPIs also measure the execution of processes. The process consists of one or more activities. To execute an activity an organization uses, creates or changes different resources. Examples of resources are people, computer components and information. KPIs are used to measure performance of activities and utilization of resources. In Fig. 2 the three concepts used in the method are highlighted in grey. When applied to the research presented in this paper, these concepts are fraud management key performance indicator (herein referred to as just KPI), fraud management activity (herein referred to as just activity) and fraud management system component (herein referred to as just FMS component or component). Just as presented in the meta-model, a KPI measures performance of one or many activities. An activity is supported with one or more FMS components. These concepts are presented in Fig. 3.

The method comprises of components that are depicted in Fig. 3. From top side, a company uses KPIs to measure performance of a certain activity (or activities), which is supported by a certain FMS component (or components). From bottom side, a FMS component is used to support a certain activity (or activities) which boosts the performance, which can be measured by a specific KPI (or KPIs). To be able to connect KPIs with activities and FMS components, we need to introduce two matrices, namely a KPI/activity matrix and an activity/FMS component matrix. In this chapter we present all five concepts that constitute our method: KPIs, KPI/activity matrix, activities, activity/FMS component matrix and FMS components.

### 3.2. Method components

From expert interviews, literature review and our own experience, first 48 key performance indicators were selected, that can be used to measure fraud management performance. Later a simplified version of 11 KPIs was introduced. These reduced set (see Table 2) can be easily calculated by any insurance company.

In Table 2 KPIs that are based on monetary values, such as "Average cost of investigation", are presented in a general form. In order to make these KPIs comparable across different time and different countries one needs to account for different currency value fluctuations. In order for the method to be useful in such setting one needs to record exact time when the KPI was collected so the currency value fluctuations can be taken into account when comparing KPIs from different points in time. In the research presented in this paper all KPIs were collected for the same year, so the correction is not needed.

**Table 2.** Simplified set of KPIs with measurement unit and calculation formula

| KPI | Unit | Formula |
|---|---|---|
| Percentage of claims investigated | Percentage | Number of investigated claims / Number of all claims |
| Detected potential fraud | Percentage | Cost of detected potential fraud / Total claims paid |
| Average investigated claim value | Currency | Cost of all investigated claims / Number of investigated claims |
| Number of clams per investigator | Number | Number of investigated claims / Number of investigators |
| Average cost of investigation | Currency | Total cost of investgation / Number of investigated claims |
| Percentage of claims in redress | Percentage | Number of claims in redress / Number of all claims |
| Success rate | Percentage | Total savings (currency) / Value of investigated claims |
| Total savings | Percentage | Total savings (currency) / Total claims paid |
| Percentage of claims in sanctioning | Percentage | Number of claims in sanctioning / Number of all claims |
| Sanctioning success rate | Percentage | Number of claims sanctioned / Number of claims in sanctioning |
| Profitability | Percentage | Total savings / Total cost of fraud management |

**Table 3.** Activities and goals of activities

| Activity | Goal |
|---|---|
| Detection | G1.1 Detect fraudulent activities as early as possible |
| | G1.2 Detect all fraud |
| | G1.3 Detect enough potential fraud for investigators |
| | G1.4 Minimize false positives |
| Prioritization | G2.1 Select the most perspective claims from detected potential |
| Investigation | G3.1 Eliminate false positives early |
| | G3.2 Investigate cases efficiently |
| | G3.3 Collect enough evidence to prove fraud |
| | G3.4 Employ effective techniques to collect evidence |
| Redress / mitigation | G4.1 Successfully recover the money / withhold the payment |
| | G4.2 Employ efficient and effective mitigation techniques |
| Sanctioning | G5.1 Prepare and submit effective criminal indictments |
| | G5.2 Help police/prosecution to achieve desired outcome |

As mentioned before, the main activities are fraud detection, prioritization, investigation, redress, mitigation and sanctioning. Each of the activities has one or more goals, which can be measured with KPIs. List of activities and their goals are provided in Table 3.

A number of different software and information system components obtained from the literature, are used to support fraud management activities. All FMS components are listed in Table 4.

The KPI/activity matrix was obtained from a correlation assessment based on expert interviews. Some KPI/activity pairs were found to be mildly correlated and some were found to be strongly correlated.

As depicted in the matrix (see Fig. 4), there are five KPI/activity pairs with a strong correlation.

1. Detected potential/Detection. The correlation is intuitive, better fraud detection activity yields more detected potential fraud.
2. Average cost of investigation/Detection. Good detection produces good detected results and the suspicion is easy to understand. Investigators spend less time trying to understand suspicions and receive less false positives; the effect is reduced average cost of investigation.
3. Average investigated claim value/Prioritization. The correlation is intuitive, as selecting the most expensive claims to investigate is one of the goals of prioritization.

**Table 4.** Fraud management system components

| Fraud Management System Component |
|---|
| System architecture |
| Expert systems |
| Classification components |
| Statistical components |
| Profiling components |
| Visual tools |
| Fraud reports |
| Automatic learning components |
| Claims database |
| ETL and data cleaning |
| Data warehouse |
| Natural language processing |
| Ranking components |
| Business process management system |

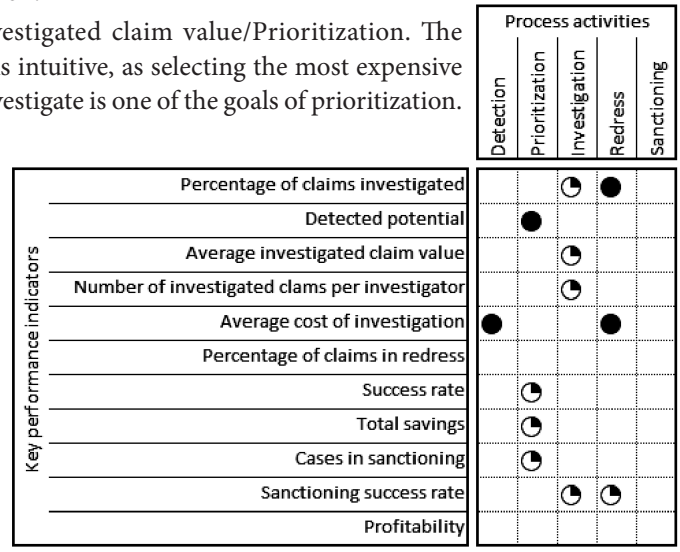


**Fig. 4.** KPI/activity matrix. Full circle denotes strong correlation, quarter circle denotes mild correlation

| Fraud Management Process Activities | | Importance (average expert rate) | System architecture | Expert systems | Classification | Statistical | Profiling | Visual tools / data mining | Fraud reports | Automatic learning | Database (Claims database) | ETL and data cleaning | Data Warehouse | Natural language processing | Ranking techniques | Business process management |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Detection | G1.1 Detect fraudulent activities as early as possible | 8,17 | ● | | | | | | | | ● | ◔ | | | | |
| | G1.2 Detect all fraud | 7,00 | | ● | ◔ | ◔ | ◔ | ◔ | ● | ○ | | | | ◔ | | |
| | G1.3 Detect enough potential fraud for investigators | 8,33 | | ◔ | ○ | ○ | ○ | ○ | ◔ | ○ | ◔ | ◔ | | | ◔ | |
| | G1.4 Minimize false positives | 6,50 | | ◔ | ◔ | | | | ◔ | ◔ | | | | | ● | |
| Prioritization | G2.1 Select the most perspective claims from detected potential | 9,17 | | ◔ | ◔ | | | | | | ○ | ○ | | | ● | |
| Investigation | G3.1 Eliminate false positives early | 6,33 | | ● | ◔ | | ◔ | ◔ | ● | | | | ◔ | | ◔ | |
| | G3.2 Investigate cases efficiently | 7,83 | | | | ◔ | ◔ | ◔ | ● | | | | ◔ | | | ◔ |
| | G3.3 Collect enough evidence to prove fraud | 7,33 | | ◔ | | | | ● | ● | | ● | ● | ● | ● | | |
| | G3.4 Employ effective techniques to collect evidence | 9,17 | | | | | | | | | | | | | | |
| Redress / mitigation | G4.1 Successfully recover the money / withhold the payment | 8,50 | | ● | | | | | ◔ | | ● | | | | | ● |
| | G4.2 Employ efficient and effective mitigation techniques | 5,67 | | | | ○ | | ○ | ◔ | | | | | | | ● |
| Sanctioning | G5.1 Prepare and submit effective criminal indictments | 6,17 | | ● | | ○ | | ○ | ● | | ◔ | ◔ | ◔ | | | |
| | G5.2 Help police/prosecution to achieve desired outcome | 7,33 | | ◔ | | ○ | | ○ | ◔ | | ● | ○ | ○ | | | ◔ |
| SUM | | | 74 | 368 | 95 | 72 | 72 | 157 | 421 | 35 | 335 | 151 | 134 | 87 | 185 | 173 |
| Relative importance | | | 3 | 16 | 4 | 3 | 3 | 7 | 18 | 1 | 14 | 6 | 6 | 4 | 8 | 7 |

**Fig. 5.** Activity/FMS component matrix represented using House of Quality. Full circle denotes strong impact, quarter circle denotes medium impact and empty circle denotes mild impact

4. Percentage of investigated claims/Redress. Companies that are able to redress the claims regularly, invest more in fraud management, and therefore investigate more claims than those who don't. On the other side, redress is one of the most time-consuming activities and when executed efficiently and effectively leaves more time to investigators to investigate more.
5. Average cost of investigation/Redress. The reason is the same as above. Redress is one of the most time-consuming activities and when executed efficiently and effectively leaves more time to investigators to investigate more claims, therefore decreasing the average cost of investigation.

Activity/FMS component matrix presents the correlation between activities and FMS components. House of Quality was used to construct and represent the correlations. In the Fig. 5, the left side of the matrix presents the activities and the particular activity goals. The next column (Importance) presents relative goal importance as marked by the experts. The top side of the matrix presents FMS components. There are circles in the matrix, which denote impact of FMS components on the activity or activity goals. For each of the FMS components, there is a relative importance at the bottom of the matrix.

As depicted in Fig. 5, the highest relative importance is attributed to the following three FMS components: (1) fraud reports, (2) expert systems and (3) claims database, and the lowest relative importance to: (1) automatic learning, (2) statistics and (3) profiling.

### 3.3. Method use case

The method should be used by practitioners to construct fraud management improvement strategies, based on the current company business performance. Company measures KPIs, compares the values to the industry average to see which KPIs could or should be improved. Then by using the proposed method, a company can evaluate which of the activities should be improved and which FMS components could aid the improvement.

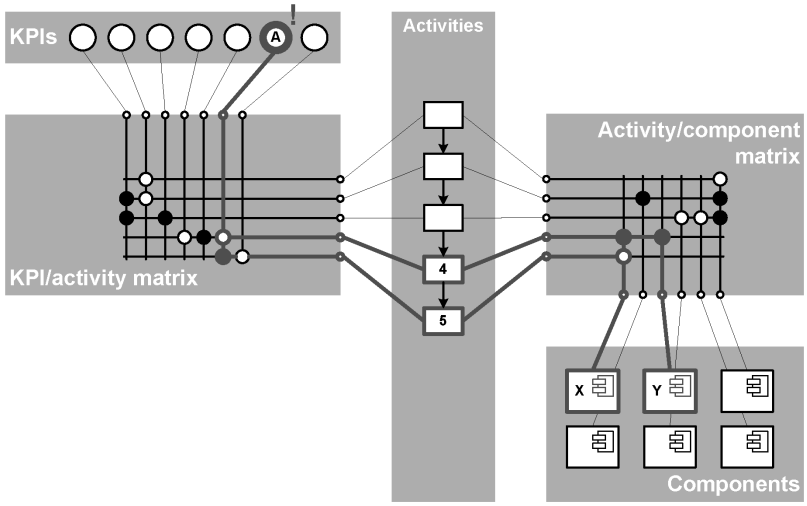


**Fig. 6.** Extended fraud management reference model can be used as a strategic tool for investment in both processes and fraud management system improvement

Fig. 6 depicts a typical use case. An insurance company notices that it underperforms on the KPI A. By using the KPI/activity matrix, the company assessed that KPI A correlates with activities 4 and 5, and by employing the activity/FMS component matrix, it can conclude that the FMS components X and Y provide the best support for activities 4 and 5. Final conclusion can be: in order to improve KPI A, the company should improve activities 4 and 5, and in order to support the activities with FMS components, components X and Y should be used.

## 4. Case study

The aim of the presented case study was to test the proposed method in a real life scenario and evaluate the KPI/activity matrix and the activity/component matrix.

The case study was conducted in three individual companies in the Slovene insurance market. As mentioned before, three additional insurance companies provided their performance KPIs and participated in assessments needed to construct the KPI/activity matrix and activity/component matrix. The case study was conducted with the following steps.

a) **Identification of improvement potential**. Three companies decided to cooperate in the case study. First, their KPIs were compared to the average Slovene industry KPIs, thus the KPIs that could be improved were identified.

b) **Components identification and improvement assessment**. Each company identified the components that would increase the performance by using the method proposed in this paper. The impact that the implementation of the proposed component should have on all KPIs, was also assessed.

c) **Results evaluation**. One year after implementation, new KPIs were collected from these three companies and compared the results to both previous performance and assessed improvement.

The companies that participated don't want their identity disclosed. Figures that would enable one to identify a concrete company are not presented in the following case study description.

### 4.1. Identification of potential improvements

The performance of three companies (later referred to as C1, C2 and C3) that participated in the case study were compared to performance from all six companied on the Slovene motor insurance market. For each of the three companies the KPIs in which the company was underperforming and could be improved substantially in relation to the industry average we identified. From the KPIs, that can be improved, the three companies selected the KPIs that they wanted to improve and assigned each KPI with improvement priority (see Table 5).

**Table 5.** Improvement priorities of selected KPIs. A number denotes the priority of improvement, 1 meaning high priority and 2 meaning lower priority

| KPI | Company | | |
|---|---|---|---|
| | C1 | C2 | C3 |
| Percentage of claims investigated [%] | | 1 | |
| Detected potential fraud [%] | 1 | | |
| Average investigated claim value [€] | | | 1 |

*Continued Table 5*

| KPI | Company | |
|---|---|---|
| Number of clams per investigator [number] | | |
| Average cost of investigation [€] | 1 | 2 |
| Percentage of claims in redress [%] | | |
| Success rate [%] | 2 | |
| Total savings [%] | 2 | |
| Percentage of claims in sanctioning [%] | | |
| Sanctioning success rate [%] | | |
| Profitability [%] | 2 | |

### 4.2. Components identification and improvement assessment

Based on the KPI improvement priorities, the proposed method was used to calculate a component match. For each of the correlation points on the matching matrices (see Figs 4 and 5) we applied the recommended (Matook and Indulska 2009) numbers 9, 3 and 1 for strong, moderate and week correlation, respectively.

**Table 6.** Component recommendations for each of the insurance companies. Lower number means higher priority. The highest priority is emphasized with green color. Second and third recomendation are highlighted with yellow color

| Component | Company | | |
|---|---|---|---|
| | C1 | C2 | C3 |
| System architecture | 6 | 9 | 7 |
| Expert systems | 1 | 3 | 3 |
| Classification | 5 | 9 | 6 |
| Statistical | 8 | 9 | 6 |
| Profiling | 10 | 10 | 5 |
| Visual tools / data mining | 8 | 5 | 2 |
| Fraud reports | 4 | 2 | 1 |
| Automatic learning | 9 | 11 | 7 |
| Database (Claims database) | 3 | 4 | 4 |
| ETL and data cleaning | 7 | 7 | 4 |
| Data Warehouse | 13 | 8 | 2 |
| Natural language processing | 12 | 9 | 4 |
| Ranking techniques | 2 | 6 | 6 |
| Business process management | 11 | 1 | 6 |

Our method predicted the most suitable components for each of the three companies (presented in Table 6). For C1 the most suitable component is an expert system (ES), followed by a ranking component and claims database. For C2, our method suggested a business process management component (PBM) as the most suitable component, followed by fraud reports and expert systems. For C3, the most suitable components in priority order were fraud reports (FR), visual (data mining) tools and data warehouse.

The implementation of a component does not only affect the KPIs selected for improvement, but has a larger footprint. With reverse use of our method, we assessed what KPIs would be affected with an implementation of a particular component. The results are presented in Table 7.

As presented in Table 7, the introduction of an expert system component should have the biggest impact on the average cost of investigation, percent of investigated claims and detected potential. Main goal for C1 was to raise detected potential and to lower the average cost of investigation, which corresponds with the predictions. The lower priority goal of C1

was also to increase total savings, the number of cases in sanctioning and profitability. As predicted with our method, the introduction of ES should also increase total savings and success rate, but our method does not predict an effect of introduction of ES to profitability. Main goal for C2 was to increase the percentage of investigated claims, and secondly to lower the average cost of investigation. This exactly concedes with the predicted effects of BPM component implementation. Main goal of C3 was to increase the average investigated claim value. As assessed with our method, the implementation of FR should have an impact on average investigated claim KPI, but not a very big one. As none of the other components had bigger impact on this particular KPI, C3 still decided to implement the FR component.

**Table 7.** Predicted and goal estimated KPI improvements for each component and insurance company. ES stands for expert system component predicted improvements, and GC1 for company 1 goal improvement. BPM and FR stands for business process management component and fraud report component, respectively. Numbers under components denote predicted improvement level, where the lower value means higher improvement. Highest predicted improvement is highlighted in green and 2nd and 3rd highest predicted improvement are highlighted in yellow. "–" means no predicted improvement

| KPI | Component | | | | | |
|---|---|---|---|---|---|---|
| | ES | GC1 | BPM | GC2 | FR | GC3 |
| Percentage of claims investigated | 2 | | 1 | 1 | 2 | |
| Detected potential | 3 | 1 | 5 | | – | |
| Average investigated claim value | 6 | | 4 | | 4 | 1 |
| Number of investigated clams per investigator | 6 | | 4 | | 4 | |
| Average cost of investigation | 1 | 1 | 2 | 2 | 1 | |
| Percentage of claims in redress | – | | – | | – | |
| Success rate | 5 | 2 | – | | – | |
| Total savings | 5 | 2 | – | | – | |
| Cases in sanctioning | 5 | | – | | – | |
| Sanctioning success rate | 4 | | 3 | | 3 | |
| Profitability | – | 2 | – | | – | |

### 4.3. Results

Companies C1, C2 and C3 implemented ES, BPM and FR components, respectively. C1 finished with implementation in 2008, C2 and C3 finished in 2009. One year after the implementation of the component, we again collected the KPIs for that year. A set of KPIs from the last company was collected in September 2010.

The results (see Table 8) are presented as a ratio of KPI value, measured after the component implementation relative to the KPI value measured before the implementation.

As depicted in the Table 8, the results for C1 were as follows. There was an improvement in all KPIs, although in some of them minimal. There was an observed improvement of more than 11.57% in all KPIs, where improvement was set as a goal. The highest relative change was in the profitability, followed by the detected potential and investigated claim value. This coincides with the goal to increase the detected potential. Companies also observed a decrease in the average cost of investigation, and an increase in success rate, total savings and profitability, set as a low-priority improvement goal. The biggest discrepancy was in the percentage

of investigated claims. The method predicted that an introduction of an ES should have a relatively high impact on that KPI, but the observed relative change was amongst the lowest.

**Table 8.** Relative change in KPI value, goal ("G") improvement KPI and predicted ("P") imrpovement KPI

| KPI | Company | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | C1 | G | P | C2 | G | P | C3 | G | P |
| Percentage of claims investigated | 5.21% | | 2 | 26.62% | 1 | 1 | –8.66% | | 2 |
| Detected potential | 62.41% | 1 | 2 | 1.33% | | | 3.25% | | |
| Average investigated claim value | 18.38% | | | –18.31% | | | 67.12% | 1 | |
| Investigated clams per investigator | 24.27% | | | 33.27% | | | –12.85% | | |
| Average cost of investigation | –20.77% | 1 | 1 | –19.35% | 2 | 2 | 17.25% | | 1 |
| Percentage of claims in redress | 6.01% | | | 12.06% | | | 8.41% | | |
| Success rate | 11.57% | 2 | | –5.38% | | | 18.10% | | |
| Total savings | 33.89% | 2 | | 18.74% | | | 42.67% | | |
| Cases in sanctioning | 0.68% | | | 1.93% | | | 0.40% | | |
| Sanctioning success rate | 23.33% | | | –1.51% | | 2 | 32.26% | | 2 |
| Profitability | 83.94% | 2 | | 34.81% | | | 49.27% | | |

In the case of company C2, a decrease in three KPIs, namely average investigated claim value, success rate and sanctioning success rate, was observed. However, there was at least 19.35% improvement in both goal KPIs. The highest relative change was in profitability, followed by the number of investigated claims per investigator and the percentage of investigated claims. The biggest surprise was to observe the difference between predicted relatively high correlation between the BPM component implementation and sanctioning success rate, however, after the experiment an actual decrease of this KPI was observed. The BPM component enabled the investigator to be more efficient and do more, without improving the detection, the pool of suspicious claims remained the same (no change in the detected potential). Because the prioritization technique of the C2 is strongly cost based, the average investigated claim value of course decreased, as well as the success rate. The observed sanctioning success rate decrease in our opinion is purely random and is not related to introduction of BPM component.

In the case of company C3, there was, a decrease in percentage of claims investigated and the number of investigated claims per investigator, and an increase of the average cost of investigation. The two mentioned KPIs are related. The highest relative change was observed ar the average investigated claim value a goal KPI, followed by profitability and total savings. As predicted with the method, the introduction of a FR resulted in a relative change in average investigation cost and sanctioning success rate, but even though the method predicted relatively high impact on percentage of investigated claims, the impact was low compared to others. With the introduction of a fraud report component, the focus of C3 switched from small frauds to large organized fraud. Such cases are more expensive and more complex. Consequently, less claims were investigated, thus a decrease in number of investigated claims, percentage of claims investigated and an increase of the average cost of investigation.

## 5. Discussion

In the case study the method was applied to three different real life scenarios. In all of the case studies, the method was used to select the appropriate component to improve the selected KPIs. All three companies implemented the proposed component and after one year of use, KPIs values were collected to compare performance before and after.

All three case studies provide positive results and prove that the proposed method works for the Slovene market. We would like to further stress that in all the case studies the implementation of proposed components produced positive improvement at the same KPIs that were set as improvement goals.

Additionally, positive and negative changes in performance were observed, which were not predicted by the method in all three cases. And more interesting, a better match with goal improvement was observed, and actual improvement, than with predicted improvement and actual improvement. Both facts arise from the same reason. It is not solely influenced by the components that are responsible for performance increase; it is also influenced by the end users, who do it by using these components. We believe that with a clear goal in mind, the users adapted the use of components to fit their concrete demands. The BPM component, for example, can generally improve efficiency of sanctioning. But if it is only used to support investigation processes and not sanctioning processes, it will not affect sanctioning at all. Therefore, the way of using of the implemented components (activities) affects the performance gained by using of the components.

As far as general performance is concerned improvement was seen in general performance, i.e. total savings (observed increase between 18.74% and 42.67%) and profitability (observed increase between 34.81% and 83.94%) in all three cases. All three implementations were seen as successful by insurance companies.

## 6. Conclusion and further work

Insurance companies have great interest in tackling insurance fraud. The research community so far offered only partial solutions, addressing particular activities of fraud management. What's more, research results in the field of insurance fraud management systems seldom are clearly linked to business level relevant performance indicator. There is a need to address the fraud management in more holistic manner and provide a clear link between fraud management system components and their effect on fraud management business performance. The paper describes a method that links fraud management system components to fraud management business performance. When companies are deciding, which business performance KPI is in need of improvement, our method enables them to learn which activities need improvement and which fraud management system component can support these activities.

The paper presents the components of the method and a use case, describing use in practice. The method was constructed based on the data gained from Slovene motor insurance companies. Three companies also tested the method by implementing the fraud management system components proposed by our method. The results are provided in the paper as a case study and based on the results the following two conclusions can be made.

Firstly, in all three case studies an increase in profitability was observed, a KPI measuring overall fraud management performance. The increase in companies C1, C2 and C3 was 83.94%, 34.81% and 49.27% respectively. It can be concluded that by improving the "right areas" with help of the method, a company can increase general performance. The "right areas" in this context means the KPIs in which the company is greatly underperforming the market.

Secondly, the improvements in all three cases appeared in the areas as desired and predicted. Exception was in sanctioning success rate at company C2. The method predicted performance increase, but in a case study an actual 1.52% decrease in performance was observed. This can be interpreted as a mild deviation, as the company C2 goal was not to increase sanctioning success rate, and it was predicted by our method as a side effect. Therefore the desired improvement of the company C2 was met. It can be concluded that by using our method a company can select fraud management system component(s), which will help them to improve the desired business performance KPIs.

Our future plan is to further improve and extend proposed method. On one side, we would like to gather KPI and performance measurements outside Slovenia to get a statistically more significant data set. We are however somewhat sceptical that international comparison will yield good results, as it disregards specifics of local environment and local insurance business environment. On the other side, our plan is to test our method in more insurance companies with purpose to improve the method. We found it relatively easy to demonstrate and show the method to insurance companies, but it is extremely hard to convince insurance companies to make real implementation of the proposed fraud management system component(s). As the side products of our method we would like to construct a fraud management performance benchmark, a set of KPIs, based on a statistically large enough measurements set, with which an individual insurance *company could compare their own performance.*

## Acknowledgements

*We wish to acknowledge and thank the three insura*nce companies; company Optilab and all the experts from the insurance companies' fraud investigation departments who helped us conduct this research.

## References

Abidogun, O. A. 2005. *Data Mining, Fraud Detection and Mobile Telecommunications: Call Pattern Analysis with Unsupervised Neural Networks:* Master thesis, University of the Western Cape.

Aggarwald, C. C.; Yu, P. S. 2005. An effective and efficient algorithm for high-dimensional outlier detection, *The VLDB Journal* 14: 211–221. doi:10.1007/s00778-004-0125-5

Artis, M.; Ayuso, M.; Guillen, M. 1999. Modeling Different Types of Automobile Insurance Fraud Behavior in the Spanish Market, *Insurance: Mathematics and Economics* 24: 67–81. doi:10.1016/S0167-6687(98)00038-9

Artís, M.; Ayuso, M.; Guillén, M. 2002. Detection of Automobile Insurance Fraud with Discrete Choice Models and Misclassified Claims, *The Journal of Risk and Insurance* 63(3): 325–340.

Barbará, D.; Domeniconi, C.; Rogers, J. P. 2006. Detecting outliers using transduction and statistical testing, in *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining.*

Barse, E. L.; Kvarnström, H.; Jonsson, E. 2003. Synthesizing Test Data for Fraud Detection Systems, in *Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC '03),* Las Vegas, Nevada, USA. IEEE Computer Society, Los Alamitos, CA, USA, 384–395.

Becker, D.; Kessler, D.; McClellan, M. 2005. Detecting Medicare abuse, *Journal of Health Economics* 24: 189–210. doi:10.1016/j.jhealeco.2004.07.002

Bermudez, L.; Perez, J. M.; Ayuso, M.; Gomez, E.; Vazquez, F. J. 2007. A Bayesian dichotomous model with asymmetric link for fraud in insurance, *Insurance: Mathematics and Economics* 42(2): 779–786. doi:10.1016/j.insmatheco.2007.08.002

Bolton, R. J.; Hand, D. J. 2002. Statistical Fraud Detection: A Review, *Statistical Science* 17: 235–249. doi:10.1214/ss/1042727940

Bonchi, F.; Giannotti, F.; Mainetto, G.; Pedreschi, I. D. 1999. A classification-based methodology for planning audit strategies in fraud detection, in *Proceedings of the fifth ACM SIGKDD international conference on knowledge discovery and data mining*.

Bond, E. W.; Crocker, K. J. 1997. Hardball and the soft touch: The economics of optimal insurance contracts with costly state verification and endogenous monitoring costs, *Journal of Public Economics* 63: 239–264. doi:10.1016/S0047-2727(96)01594-0

Bordoni, S.; Facchinetti, G. 2001. Insurance Fraud Evaluation: A Fuzzy Expert System, in *FUZZ-IEEE*, 1491–1494.

Boukerche, A.; Juc, K. R. L.; Sobral, J.; B.; Notare, M. S. M. A. 2004. An artificial immune based intrusion detection model for computer and telecommunication systems, *Parallel Computing* 30: 629–646. doi:10.1016/j.parco.2003.12.008

Brockett, P. L.; Derrig, R. A.; Golden, L. L.; Levine, A.; Alpert, M. 2002. Fraud Classification using Principal Component Analysis of RIDITs, *The Journal of Risk and Insurance* 69(3): 341–371. doi:10.1111/1539-6975.00027

Cahill, M. H.; Lambert, D.; Pinheiro, J. C.; Sun, D. X. 2002. *Detecting Fraud in Real World*. Handbook of Massive Data Sets, Kluwer Academic Publishers, 913–930.

Caron, L.; Dionne, G. 1999. Insurance Fraud Estimation; More Evidence From the Quebec Automobile Insurance Industry, in Dionne, G. and Laberge-Nadeau, C. (Eds.). *Automobile Insurance: Road Safety, Nexv Drivers, Risks, Insurance Fraud and Regulation*, Kluwer, 175–182.

Chang, R.; Ghoniem, M.; Kosara, R.; Ribarsky, W.; Yang, J.; Sumak, E.; Ziemkiewicz, C.; Kern, D.; Sudjianto, A. 2007. WireVis: Visualization of Categorical, Time-Varying Data From Financial Transactions, in *IEEE Symposium on Visual Analytics Science and Technology 2007*. Sacramento, California, USA. IEEE Computer Society, Los Alamitos, CA, USA, 155–162.

Cox, K. C.; Eick, S. G.; Wills, G. J.; Brachman, R. J. 1997. Visual data mining: recognizing telephone calling fraud, *Data Mining and Knowledge Discovery* 1(2): 225–231. doi:10.1023/A:1009740009307

Curet, O.; Jackson, M.; Tarar, A. 1996. Designing and evaluating a case-based learning and reasoning agent in unstructured decision making, in *IEEE International Conference on Systems, Man, and Cybernetics, 1996*, Beijing, China. IEEE Computer Society, Los Alamitos, CA, USA, 2487–2492.

Derrig, R. A.; Weisberg, H. I.; Chen, X. 1994. Behavioral Factors and Lotteries Under No-Fault with a Monetary Threshold: A Study of Massachusetts Automotive Claims, *Journal of Risk and Insurance* 61(2): 245–275. doi:10.2307/253710

Derrig, R. A. 2002. Insurance Fraud, *The Journal of Risk and Insurance* 69(3): 271–287. doi:10.1111/1539-6975.00026

Dionne, G.; Giuliano, F.; Picard, P. 2009. Optimal Auditing with Scoring: Theory and Application to Insurance Fraud, *Management Science* 55(1): 58–70. doi:10.1287/mnsc.1080.0905

Eriksson, H. E.; Penker, M. 2000. *Business Modelling with UML: Business Patterns at Work*. John Wiley & Sons.

Fawcett, T.; Provost, F. 1997. *Adaptive Fraud Detection*. Data Mining and Knowledge Discovery, Kluwer.

Fawcett, T.; Provost, F. 1999. Activity monitoring: noticing interesting changes in behaviour, in *Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining,* 1999, San Diego, California, USA. ACM, New York, USA, 53–62.

Furlan, Š.; Bajec, M. 2009. Praksa slovenskih avtomobilskih zavarovalnic pri razreševanju zavarovalniških goljufij, *Zavarovalniški horizonti* 5(3): 29–41.

Garner, B.; Chen, F. 1994. Hypothesis Generation Paradigm for Fraud Detection, in *Proceedings of 1994 TENCON '94. IEEE Region 10's Ninth Annual International Conference. Theme: Frontiers of Computer Technology*, Singapore. IEEE Computer Society, Los Alamitos, CA, USA, 197–201.

Gudas, S. 2009. Enterprise knowledge modelling: domains and aspects, *Technological and Economic Development of Economy* 15(2): 281–293. doi:10.3846/1392-8619.2009.15.281-293

Gudmundsson, S.; Oddsdottir, G. L.; Runarsson, T. F.; Sigurdsson, S.; Kristjansson, E. 2010. Detecting fraudulent whiplash claims by support vector machines, *Biomedical Signal Processing and Control* 5(4): 311–317. doi:10.1016/j.bspc.2010.05.004

Hauser, J. R.; Clausing, D. 1988. The House of Quality, *Harvard Business Review* 3: 63–73.

He, H.; Wang, J.; Graco, W.; Hawkins, S. 1997. Application of Neural Networks to Detection of Medical Fraud, *Expert Systems with Applications* 13(4): 329–336. doi:10.1016/S0957-4174(97)00045-6

Hollien, H.; Geison, L.; Hicks, J. W. 1987. Voice stress analysis and lie detection, *Journal of Forensic Sciences* 32(2): 405–418.

Hyman, D. A. 2002. HIPAA and Health Care Fraud: An Empirical Perspective, *Cato Journal* 22(1): 151–178.

Jonas, J. 2006. Threat and fraud intelligence, Las Vegas style, *IEEE. Security and Privacy* 4(6): 28–34. doi:10.1109/MSP.2006.169

Jou, S.; Hebenton, B. 2007. Insurance fraud in Taiwan: Reflections on regulatory effort and criminological complexity, *International Journal of the Sociology of Law* 35: 127–142. doi:10.1016/j.ijsl.2007.04.002

Kalibatiene, D.; Vasilecas, O. 2010. Ontology axioms for the implementation of business rules, *Technological and Economic Development of Economy* 16(3): 471–486. doi:10.3846/tede.2010.29

Ko, R. K. L. 2009. A Computer Scientist's Introductory Guide to Business Process Management (BPM), *ACM Crossroads* 15(4): 11–18. doi:10.1145/1558897.1558901

Lavbič, D.; Vasilecas, O.; Rupnik, R. 2010. Ontology based multi-agent system to support business users and management, *Technological and Economic Development of Economy* 16(2): 327–347. doi:10.3846/tede.2010.21

Lundin, E.; Kvarnström, H.; Jonsson, E. 2002. A Synthetic Fraud Data Generation Methodology, in *Proceedings of the 4th International Conference on Information and Communications Security* (ICICS '02), London, UK. Springer-Verlag, UK, 265–277.

Major, J.; Riedinger, D. R. 2002. EFD: A Hybrid Knowledge/Statistical-Based System for the Detection of Fraud, *The Journal of Risk and Insurance* 69(3): 309–324. doi:10.1111/1539-6975.00025

Matook, S.; Indulska, M. 2009. Improving the quality of process reference models: A quality function deployment-based approach, *Decision Support Systems* 47: 60–71. doi:10.1016/j.dss.2008.12.006

Mattison, R. 2005. *The Telco Revenue Assurance Handbook*. XiT Press, Oakwood Hills, Illinois, USA.

Ngai, E. W. T.; Yong, Hu; Wong, Y. H.; Yijun Chen; Xin Sun. 2010. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature, *Decision Support Systems*. doi:10.1016/j.dss.2010.08.006

Nguyen, T. M.; Schiefer, J.; Tjoa, A. M. 2005. Sense & Response Service Architecture (SARESA): An Approach towards a Real-time Business Intelligence Solution and its use for a Fraud Detection Application, in *Proceedings of the 8th ACM international workshop on Data warehousing and OLAP* (DOLAP '05), New York, USA. ACM, New York, 77–86.

NHS. 2001. *Countering Fraud in the NHS* [online] National Health Service (Published 2001), [accessed 28 May 2010]. Available from Internet: <http://www.nhsbsa.nhs.uk/fraud>.

NHS. 2006a. *Creating an Anti-Fraud Culture: Discovering the Public's Perception of Fraud in the NHS* [online] National Health Service (Published 2006), [accessed 28 May 2010]. Available from Internet: <http://www.nhsbsa.nhs.uk/fraud>.

NHS. 2006b. *The International Fraud and Corruption Report: A study of selected countries* [online] National Health Service (Published 2006), [accessed 28 May 2010]. Available from Internet: <http://www.nhsbsa.nhs.uk/fraud>.

NHS. 2007. *Countering Fraud in the NHS: Applying Appropriate Sanctions Consistently* [online] National Health Service (Published 2007), [accessed 28 May 2010]. Available from Internet: <http://www.nhsbsa.nhs.uk/fraud>.

Peng, F.; McCallum, A. 2006. Information extraction from research papers using conditional random fields, *Information Processing and Management* 42(4): 963–979. doi:10.1016/j.ipm.2005.09.002

Peng, Y.; Kou, G.; Sabatka, A.; Chen, Z.; Khazanchil, D.; Shi, Y. 2006. Application of Clustering Methods to Health Insurance Fraud Detection, in *2006 International Conference on Service Systems and Service Management*, Troyes, France. Institute of Information Science, Technology & Engineering, Nebraska University, Omaha, NE, 116–120.

Poibeau, T.; Kosseim, L. 2001. Proper-name Extraction from Non-Journalistic Texts, *Language and Computers* 37: 144–157.

Popowich, F. 2005. Using Text Mining and Natural Language Processing for Health Care Claims Processing, in *SIGKDD Explorations* 7(1): 59–66.

Phua, C.; Alahakoon, D.; Lee, V. 1998. Minority Report in Fraud Detection: Classification of Skewed Data, *SIGKDD Exploration* 6(1): 50–59.

Phua, C.; Lee, V.; Smith, K.; Gayler, R. 2005. A Comprehensive Survey of Data Mining-based Fraud Detection Research, *Artificial Intelligence Review*.

Radcliffe, J. G. Y. 1995. The Insurance Industry's Use of Database to Prevent and Detect Fraud, and Improve Recoveries, in *European Convention on Security and Detection,* Brighton, UK. IEE, 216–224.

Schiller, J. 2006. The Impact of Insurance Fraud Detection Systems, *Journal of Risk and Insurance* 73(3): 421–438. doi:10.1111/j.1539-6975.2006.00182.x

Selinšek, L. 2004. Kazenskopravni vidiki zavarovalniških goljufij – nekatera izhodišča, *Goljufije v zavarovalništvu*, 89–106.

Silverstone, H.; Davia, H. R. 2005. *Fraud 101: Techniques and Strategies for Detection*. 2nd ed. Wiley.

Sokol, L.; Garcia, B.; West, M.; Rodriguez, J.; Johnson, K. 2001. Precursory Steps to Mining HCFA Health Care Claims, in *Proceedings of the 34th Hawaii International Conference on System Sciences*, Hawaii, USA. IEEE Computer Society, Los Alamitos, CA, USA, 6019–6029.

Stempel, J. W. 2002. Recent Court Decisions, *The Journal of Risk and Insurance* 69(3): 245–257. doi:10.1111/1539-6975.00006_2

Sternberg, M.; Reynolds, R. G. 1997. Using Cultural Algorithms to Support Re-Engineering of Rule-Based Expert Systems in Dynamic Performance Environments: A Case Study in Fraud Detection, *IEEE Transactions on Evolutionary Computation* 1(4): 225–243. doi:10.1109/4235.687883

Stolfo, S. J.; Fan, W.; Lee, W. 2000. Cost-based modeling for fraud and intrusion detection: results fromthe JAM project, in *DARPA Information Survivability Conference and Exposition* (DISCEX'00), South Carolina, USA. IEEE Computer Society, Los Alamitos, CA, USA, 130–144.

Sun, Z.; Finnie, G. 2004. Experience based reasoning for recognising fraud and deception, in *Proceedings of the Fourth International Conference on Hybrid Intelligent Systems (HIS'04)*, Kitakyushu, Japan. IEEE Computer Society, Los Alamitos, CA, USA, 80–85.

Tennyson, S.; Salsas-Forn, P. 2002. Claims Auditing in Automobile Insurance: Fraud Detection and Deterrence Objectives, *The Journal of Risk and Insurance* 69(3): 289–308. doi:10.1111/1539-6975.00024

Tie, R. 2010. *SARs can Help Put Fraudsters Behind Bars 1*. Fraud Magazine.

TMF, 2006. *Revenue Assurance Guidebook* [pdf]. TeleManagement Forum Revenue Assurance Technical Team.

Tuyls, K. 2000. *Machine Learning Techniques for Fraud Detection*. Master thesis, VUB.

Viaene, S.; Derrig, R. A.; Baesens, B.; Dedene, G. 2002. A Comparison of State-of-the-Art Classification Techniques for Expert Automobile Insurance Claim Fraud Detection, *The Journal of Risk and Insurance* 69(3): 373–421. doi:10.1111/1539-6975.00023

Viaene, S.; Derrig, R. A.; Dedene, G. 2004. A Case Study of Applying Boosting Naive Bayes to Claim Fraud Diagnosis, in *IEEE Transactions on Knowledge and data Engineering* 16(5): 612–620.

Viaene, S.; Dedene, G.; Derrig, R. A. 2005. Auto claim fraud detection using Bayesian learning neural networks, *Expert Systems with Applications* 29: 653–666. doi:10.1016/j.eswa.2005.04.030

Viaene, S.; Ayuso, M.; Guillen, M.; Gheel, D. V.; Dedene, G. 2007. Strategies for Detecting Fraudulent Claims in the Automobile Insurance Industry, *European Journal of Operational Research* 176(1): 565–583. doi:10.1016/j.ejor.2005.08.005

Weisberg, H. I.; Derrig, R. A. 1998. Quantitative Methods for Detecting Fraudulent Automobile Bodily Injury Claims, *Risques* 35: 75–101.

Xing, D.; Girolami, M. 2007. Employing Latent Dirichlet Allocation for Fraud Detection in Telecommunications, *Pattern Recognition Letters* 28(13): 1818–1824.

Žagar, T. 2008. *Doprinos vizualizacije pri bolju z goljufijami v telefonskih sistemih*. Masters thesis, University of Ljubljana.

## TRANSPORTO PRIEMONIŲ DRAUDIMO APGAVYSČIŲ VALDYMO SISTEMOS KOMPONENTŲ PASIRINKIMO METODAS, GRINDŽIAMAS VERSLO VEIKLOS EFEKTYVUMU

**Š. Furlan, O. Vasilecas, M. Bajec**

**Santrauka.** Apgavystės transporto priemonių draudimo srityje lemia draudimo kompanijų nuostolius, kurie vertinami 100 milijardų dolerių per metus. Dėl to apgavysčių valdymo srityje atliekama nemažai tyrimų, tačiau daugumoje iš jų nagrinėjamos tik dalinės problemos ir daromos prielaidos, kad apgavysčių valdymo veiklos rūšys nepriklauso viena nuo kitos. Apgavysčių valdymo sistemų komponentų tyrimai retai tiesiogiai siejami su jų įtaka verslo veiklos efektyvumui. Tai lemia dažną problemą, kuri būdinga praktiniam apgavysčių valdymo sistemų naudojimui: tik nedaug draudimo kompanijų gali objektyviai įvertinti, kuris iš daugelio apgavysčių valdymo sistemų komponentų, siūlomų tyrėjų ir pardavėjų, padėtų jiems išspręsti problemas, susijusias su apgavysčių valdymu. Darbe siūlomas metodas, kuris gali būti panaudotas kaip strateginė priemonė, skirta apgavysčių valdymo procesui patobulinti transporto priemonių draudimo kompanijose. Metodas sukurtas taip, kad galėtų būti naudojamas apgavysčių valdymo sistemų komponentams pasirinkti remiantis verslo veiklos efektyvumu. Pradiniai metodo naudojami duomenys yra svarbiausių veiklos efektyvumo rodiklių, kuriuos kompanijos nori patobulinti, rinkinys. Rezultatas yra veiklos rūšių, kurios turėtų būti patobulintos, rinkinys ir apgavysčių valdymo sistemos komponentų rinkinys, kuris turėtų būti panaudotas sprendžiant suformuluotą apgavysčių valdymo uždavinį. Straipsnyje aprašytas pasiūlytas metodas ir siūlomi naudoti sistemos komponentai. Metodą realizuojantys komponentai buvo sukurti remiantis duomenimis, kurie gauti iš Slovėnijos transporto priemonių draudimo kompanijų. Pasiūlytas metodas ir jį įgyvendinanti sistema buvo išbandyti atliekant tris praktinius eksperimentus, kurių rezultatai pateikti straipsnyje.

**Reikšminiai žodžiai:** apgavysčių valdymas, apgavysčių valdymo sistemos, apgavysčių valdymo sistemų kūrimas, verslo veiklos efektyvumas, svarbiausi veiklos efektyvumo rodykliai, transporto priemonių draudimas.

**Štefan FURLAN.** Is a researcher and a PhD student at the Laboratory for Data Technologies, at the Faculty of Computer and Information Sciences at the University of Ljubljana and a CEO of Optilab. He finished his bachelors' degree before time and first in his year. For his bachelors' thesis he received the highest possible grade and a national reward (Prešernova nagrada). He is constantly improving his skills and knowledge academically and also through programs such as Center for Entrepreneurship and Executive Development. His work revolves around fraud management, fraud detection and prevention, with focus on the insurance industry. He tends to work on research that has strong practical tendency. He is also interested in innovation and start-ups and is often invited to speak about these topics. He is a member of several communities such as Slovenian Society Informatica, American Risk and Insurance Association, GI and CEED Global.

**Olegas VASILECAS.** Prof. Dr (hp). Olegas Vasilecas is full time professor at the information systems department, and senior researcher and head of Information Systems Research Laboratory in Vilnius Gediminas Technical University (VGTU). He is author of more than 200 research papers and 5 books in the field of information systems development. His research interests: knowledge, including business rule and ontology, based information systems development. He delivered lectures in 7 European universities including London, Barcelona, Athens, Valencia and Ljubljana. O. Vasilecas carried out an apprenticeship in Germany, Holland, China, and last time in Latvia and Slovenia universities. He supervised 7 successfully defended doctoral theses and now is supervising 5 doctoral students more. He was leader of many international and local projects. Last time he leaded VGTU part of "Business Rules Solutions for Information Systems Development (VeTIS)" project carried out under national High Technology Development Program.

**Marko BAJEC.** Prof. Dr Marko Bajec was born on December 6, 1970 in Postojna. After finishing secondary school on computer engineering he entered Faculty of Computer and Information Science, where he received his Diploma, Master degree and PhD degree in 1996, 1998, and 2001 respectively. Since then he works in the Department for informatics and delivers undergraduate and postgraduate courses on Information Systems and Databases. Since 2009 he is on the position of an Associative Professor. His main research interests include: software development methodologies (specifically Situational Method Engineering), IT/IS strategy planning, and software equality. Marko Bajec is also a head of the Laboratory for Data Technologies which specialises for data visualization, presentation, integration, and analysis. Marko Bajec publishes his research findings in domestic and international conferences and journals.