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

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 threat, 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