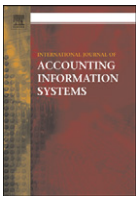
International Journal of Accounting Information Systems 9 (2008) 82–93

Contents lists available at ScienceDirect

International Journal of Accounting Information Systems



X-raying Segregation of Duties: Support to illuminate an enterprise's immunity to solo-fraud

Ph.I. Elsas *

14 rue des Algonquins, Aylmer, Quebec, Canada J9J 1A7

ARTICLE INFO

Article history:
Received 15 June 2007
Received in revised form 15 October 2007
Accepted 31 October 2007

Keywords:
Segregation of Duties
Separation of Duties
Authorization
Access Control
Internal Control
Internal Control over Financial Reporting
Assessment of the Effectiveness of Internal Control over Financial Reporting
Potential Fraud
Potential Fraud Detection

ABSTRACT

This paper presents an application of an automated scientific method to measure the quality of the design of Segregation of Duties, also known as Separation of Duties (SoD). The automated method enables an auditor to map out a body of authorizations and X-ray it on SoD. The body of authorizations is shaped by the so-called enterprise value cycle, or supercycle. The method supports an integral, top–down, diagram-based approach, including all automated and non-automated parts of an enterprise.

Input is an enterprise supercycle diagram with authorizations and abilities. Output is an overview of all potential single-employee fraud constructs, also called potential solo-frauds, that are able to undetectably subtract value from the enterprise. As remediation the automated method indicates which authorization restrictions are minimally required to create a SoD in which solo-fraud is impossible. This paper is the first publication of this method in the international scientific Accounting and Auditing community.

1. Introduction

The scientific method to measure the quality of the design of SoD was developed during the period 1990 to 1996 in a special co-operation between Deloitte Touche Tohmatsu International and the department of Mathematics and Computer Science of the *Vrije Universiteit* in the Netherlands. The method is based on Dutch auditing theory and founded in mathematical logic. It has been published in the international scientific Computer Science community and was awarded the Alfred Coini prize for the best publication in

* Tel.: +1 819 778 2720.
E-mail address: PhilipElsas@ComputationalAuditing.com.

1467-0895/$ – see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.accinf.2007.10.005

auditing, see Elsas et al. (1998) and Elsas (1996). In Elsas (1996) the method is presented in the context of a specially developed computational auditing theory, a system blueprint and a concise summary of Deloitte's Smart Audit Support – currently part of "The Deloitte Audit" – software to support audit planning; compare to Boritz and Wensley (1996). Elsas et al. (1998) focus on the SoD method and introduce it in relation to the Clark–Wilson Integrity model, see Clark and Wilson (1987). The scientific method was automated and made suited for industrial practice between 2003 and 2007. Recently there is quite some interest for the automated method, see van Wijngaarden (2007), Veenstra (2007), Elsas (2007), Ernst & Young (2006), Blokdijk (2006), Veenstra and Heertje (2006), Elsas et al. (2006), Blokdijk and Elsas (2004) and the Dutch Tax Office (2003). Background material can be found in Griffioen et al. (2000), Blokdijk et al. (1995), Elsas et al. (1992), Frielink and De Heer (1985–1989), Reisig (1985) and Burgert (1957). For more approaches see Hendrawirawan et al. (2007), Brooks and Lanza (2006) and Lightle and Waller Vallerio (2003).

The goal of SoD is to reduce the potential damage from the actions of one employee. Therefore, no single employee should have control over a critical combination of business transactions, critical in the sense that it offers opportunity of *undetectable* business value subtraction. SoD hinders fraud by requiring collusion: no employee should be able to commit fraud without involving another person.

Some common guiding principles in SoD design are:

1. Every employee should be authorized to a limited number of business (sub-) transactions, in a limited scope;
2. Employees should have non-coinciding, preferably opposite interests;
3. Custody, operation, registration, checking and direction are preferably in different hands.

SoD is a crucial Internal Control, that once inadequately applied cannot afterwards be compensated for by any effort of an external auditor, see Blokdijk (2004), in particular pp. 189–190. SoD is a crucial Internal Control (IC), especially when considered over Financial Reporting (ICoFR), and is commonly considered the most difficult and sometimes the most costly control to achieve.

Currently there is a layered focus regarding assessment of SoD: management's assessment of the effectiveness of ICoFR and the auditor's related assessment thereof (Sarbanes–Oxley, Section 404). For these assessments there are guidelines for the external auditor and for management, published by the U.S. Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB). During an annual financial statements audit or an audit of ICoFR, the auditor judges the degree to which an organization is fraud-proof. The audit is carried out in such a way that material fraud is exposed, excluding collusion and "management overriding", see International Standard on Auditing (ISA) 240, paragraphs 17–20: "Inherent Limitations of an Audit in the Context of Fraud".

The SEC has recently published a Concept Release concerning Management's Reports on ICoFR, File: S7-11-06. By publishing this file the SEC sought input from the public that provided helpful insights about guidance needed by management. Question 28 was: "How have companies been able to use technology to gain efficiency in evaluating the effectiveness of IC?". Reactions show consensus among auditors about a solution direction, see for example Deloitte's reaction, p.2. That direction is: development of guidance and support for management about how to perform an assessment of ICoFR. The support objectives are: effective, scalable and cost-efficient, to result in increased consistency in management's use of a top–down, risk-based approach to designing, documenting and testing of ICoFR. And, it would also enable the auditor to better apply a top–down, risk-based approach to the audit of ICoFR and to use management's testing (to the extent permitted).

A challenge well-known to auditors regarding ICoFR is Internal Control in Enterprise Resource Planning (ERP) systems, especially SoD in ERP, like SAP. When analyzing SoD one however *cannot* restrict oneself to a stand-alone analysis of authorizations within a specific system. One has to take into account authorizations in *other* systems, and one also has to take into account authorizations that are *not automated* at all. To review enterprise authorizations the auditor has to *unify* for each individual *all automated and non-automated* authorizations. Therefore, a unifying *convention*, or even better a unifying *model*, is required. The method demonstrated here offers such a unifying model.

Although audit literature has no codified system of standards for SoD that is usable as a normative framework for a scientific method, audit literature makes strong recommendations that one may consider standards (see, for example, Starreveld et al.). One important "standard" is clear: ensure there is SoD whenever it is technically and commercially feasible. There is one limitation lurking there: the limited