Aufdeckung von SoD Risiken in internen Kontrollsystemen (IKS)

Interne Kontrollsysteme (IKS) werden durch die gesteigerten Erwartungen an Compliance heutzutage immer wichtiger. Risiken zu bewerten und zu minimieren war und ist ein Problem für Unternehmen und Verwaltungen. Die Folgen sind Fehler- und Betrugsrisiken. Die strikte Trennung von Berechtigungen aufgrund der Benutzertätigkeit, auch Segregation of Duties (SoD) genannt, gewinnt an Bedeutung, was die aktuellen Vorhaben im Bereich eGovernment beweisen. Die auf Identity & Access Management (IAM) spezialisierte Firma WIB Solutions AG hat die existierende Prüfungscheckliste für IKS weiter entwickelt, um weitere und tiefere Analysen zu möglichen.

Daniel Kappeler
ICT Consultant
WIB Solutions AG
dkappeler@wib.ch

Einleitung

In einer deutschen Firma wurden Löhne über mehrere Jahre an einen Mitarbeiter ausgezahlt, den es nie gab. Der Fall, dessen Ursache in fehlenden SoD-Regeln zu finden ist, wurde unter dem Namen «Der Mann, der niemals lebte» bekannt (Bungartz 2013).

Das interne Controlling ist ein Prozess, der von der Geschäftsleitung entwickelt, implementiert und bedient wird und folgende Ziele verfolgt: (Pfaff & Ruud 2013, p.21):

- Effizienz der Geschäftstätigkeit (Operations)
- Zuverlässigkeit der finanziellen Berichterstattung (Reporting)
- Einhaltung der anwendbaren Normen (Compliance)

Die Komplexität und Anwendbarkeit von SoD in heutigen IT-Systemen bereitet vielen Organisationen Mühe (Ernst & Young 2010, p.2). SoD definiert eine Schlüsselkompetenz, die nicht einfach zu erreichen ist (Business Strategy Inc. 2010, p.3). Die angemessene Trennung der Funktionen mittels Bereitstellung von Rollen in verschiedenen Prozessschritten und Prüfung der durchgeführten Arbeiten (Business Strategy Inc. 2010, p.3) reduziert aber die Wahrscheinlichkeit von Fehlern. Das Ziel von SoD ist die Reduktion von Gelegenheiten, die zu Betrugssituationen führen können (Weaver 2012, p.1).
Die Funktionstrennung bietet vier wesentliche Vorteile:

- Minimierung des Betrugsrisikos
- Reduktion der Fehleranfälligkeit durch Früherkennung
- Dezimierung der Kosten von Korrekturmassnahmen durch Fehler-Früherkennung
- Imagesteigerung der Organisation durch Einsatz eines SoD-Prüfsystems (Business Strategy Inc. 2010, p.3).

Die Organisationen müssen keine komplexen Rollenstrukturen oder teuren Systeme einkaufen, um die SoD-Regulierungen zu erfüllen. Ein Fokus auf die Prozesse, welche die grössten Risiken beinhalten, reicht normalerweise aus (Ernst & Young 2010, p.3). Nur durch die Betrachtung von SoD als Framework oder interne Kontrolle können die Compliance-Anforderungen erfüllt werden (Ernst & Young 2010, p.4).

Ausgangslage

Pfaff & Ruud (2011) haben eine nützliche, 160 Fragen umfassende Checkliste zur Bewirtschaftung interner Kontrollen veröffentlicht.
Sie enthält folgende Informationen:

- Frage / Risikobeurteilung: Frage zu potenziellen Risiken
- Risikobetroffenheit für die Organisation (Ja/Nein)
- Sonstige Bemerkungen: zusätzliche Notizen zum Risiko

Anmerkung

Da die ursprüngliche Liste in diesem Artikel zu umfangreich wäre, werden nur die Fragen aufgeführt, welche eine hinreichende SoD-Relevanz aufweisen (siehe Grafik 1: Risikoidentifikation und Bewertung). Diese Liste ist in folgenden Aspekten unvollständig:

- Einfluss und Bewertung von Risiken
- Eintrittswahrscheinlichkeit
- Verantwortlichkeiten und Auswirkungen auf IT Systeme

WiB Solutions AG hat 160 Fragen auf ihre SoD-Relevanz überprüft, bewertet und abgestimmt. Das Ziel war, ein in der Praxis handhabbares Werkzeug zu erhalten, welches zu aussagekräftigen Antworten bei SoD-Fragen verhilft.
Folgende Kriterien wurden dabei berücksichtigt:

- Funktionstrennung
- Vier-Augen-Prinzip
- Verantwortlichkeit/Zuständigkeit
- Funktionen
- Mehrfachzahlung

Anschliessend wurden diejenigen Fragen von der Liste gestrichen, welche eine zu geringe SoD-Relevanz oder ein zu geringes Risikominimierungspotenzial aufweisen. Das Resultat sind zwölf Fragen, welche eine effektive SoD-Analyse ermöglichen.
Danach wurden die folgenden Kriterien zur Beurteilung der SoD-Risiken beigefügt:

- Relevanz SoD
- Eintrittswahrscheinlichkeit
- Schadenausmass (finanziell und/oder Imageverlust)
- Schadensbereich (Workflows, Tools, Systeme …)
- Zuständigkeiten (betroffene Stellen, Risikokontrolle …)

Vorgehen

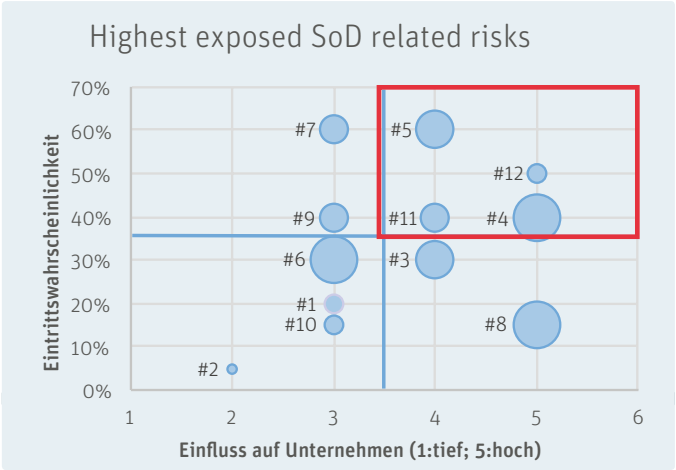
1. Risikoidentifikation

Zunächst wird eine Risikobetrachtung der zu untersuchenden Organisation durchgeführt. Hierfür werden die zwölf Fragen für den Untersuchungsbereich beantwortet und bewertet. Beispielsweise benötigt der Prozess im Rechnungswesen verschiedene Funktionen und eine klare Funktionstrennung, um Betrug vorzubeugen. Ohne SoD-Regulierungen ist es beispielsweise möglich, dass dieselbe Person Rechnungen erhält, prüft und die Geldbeträge transferiert. So könnte beispielsweise ein/e Mitarbeiter/in einen Laptop bestellen und die Rechnung unbemerkt durch die Firma bezahlen. Zur Betrugsvorbeugung ist ein aktuelles, internes Kontrollsystem notwendig, welches die Trennung verschiedener Funktionen definiert.

Die Tabelle illustriert ein Beispiel für die Risikobetrachtung mithilfe der überarbeiteten Liste (siehe Seite 37 unten).

2.Aufdeckung potenzieller Risiken

Von einer komplett ausgefüllten Vorlage wird ein Risikograph, basierend auf den wichtigsten Faktoren, erstellt, um die wesentlichsten Massnahmenfelder und damit ein optimales Vorgehen zu definieren.



Grafik 2: Matrix SoD-Risiken

Die X-Achse definiert den Einfluss auf die Organisation bei Ereigniseintritt, die Y-Achse die Wahrscheinlichkeit des Ereigniseintritts. Die Kreise stellen die gemäss Checkliste nummerierten Risikofelder dar, je grösser, desto relevanter für SoD. Der Risikograph zeigt somit die kritischen Faktoren aus Sicht SoD. Die Punkte im roten Quadrant stellen das grösste Risiko dar (grösstes Schadensausmass und grösste Eintrittswahrscheinlichkeit).

3.Massnahmendefinition

Anschliessend werden in der Reihenfolge der Risikogewichtung Massnahmen definiert. Der Berater beginnt mit den grössten Kreisen im roten Quadranten. Durch dieses Vorgehen werden die Hauptrisiken innert kürzester Zeit minimiert bzw. eliminiert.

Das Resultat ist ein in der Organisation etabliertes Risikomanagement, welches das Fehler- und Betrugspotenzial minimiert.

Schlussfolgerung

Da das Risikobewusstsein in Organisationen steigt, gewinnen interne Kontrollsysteme und eine saubere Trennung von Funktionen an Wichtigkeit. Die Lösungen sind nicht standardisierbar, da jede Situation individuell betrachtet werden muss. Eine korrekte Bewertung der Risiken und die Definition zielführender Massnahmen minimieren die Risiken und erfüllen die Anforderungen an die interne Compliance und an externen Rahmenbedingungen (Gesetze, Kunden- und Lieferantenrichtlinien etc.).

So wichtig das Thema SoD ist: Die Erstellung einer SoD-Analyse erfordert viel Erfahrung. Deshalb ist die Konsultation einer Beratungsfirma, z.B. der WIB Solutions AG, sinnvoll.

Quellen

- Bungartz, O., 2013, Der Mann, der niemals lebte – interne Kontrollsysteme im Personalwesen. Lohn+Gehalt Fachmagazin.
- Business Strategy Inc., 2010, Generic Segregation of Duties Policy.
- Ernst & Young, 2010, A risk-based approach to segregation of duties., (May).
- Pfaff, D. & Ruud, F., 2011, Anhang 3 Prüfungscheckliste – Schweizer Leitfaden zum Internen Kontrollsystem (IKS)., (1999), S. 121–136.
- Pfaff, D. & Ruud, F., 2013, Schweizer Leitfaden zum Internen Kontrollsystem (IKS) 6th ed., Orell Füssli.
- The Certified Accountant, 2009, The Fraud Triangle and What You Can Do About It. The Certified Accountant.
- Weaver, B. D., 2012, A Look at Segregation of Duties for Small Business. , (April), S. 30–31.

Nr.	Frage/Risikobeurteilung	Einfluss auf Unternehmen (1: tief; 5: hoch)	Eintrittswahrscheinlichkeit	Relevanz SoD	Zuständige Person oder Organisation	Einwirkung auf IT-Systeme
#1	Aufbauorganisation: Sind die Verantwortlichkeiten eindeutig geregelt und schriftlich festgehalten?	3	20%	2	Management	Alle IT-Systeme
#2	Aufbauorganisation: Gibt es Stellen- oder Funktionsbeschreibungen (Aufgaben, Verantwortungsbereich, Stellvertretung)?	2	5%	1	Management	Alle IT-Systeme
#3	Ablauforganisation: Berücksichtigen die Arbeits- oder Dienstanweisungen in ausreichendem Masse das Vier-Augen-Prinzip oder sonstige Kontrollen?	4	30%	4	Compliance/IKS	Alle IT-Systeme
#4	Rechnungswesen: Liegt eine Beschreibung der Funktionstrennung (Belegerstellung, Dateneingabe, Zahlungsverkehr) vor?	5	40%	5	Management/Finanz-system/Rechnungswesen	ERP-System
#5	Liquide Mittel: Ist insbesondere eine Kassenführungsordnung vorhanden?	4	60%	4	Finanzsystem	ERP-System
#6	Liquide Mittel: Besteht eine Funktionstrennung von anderen nicht zu vereinbarenden Tätigkeiten (z.B. Buchen)?	3	30%	5	Finanzsystem	ERP-System
#7	Vorräte: Gibt es eine schriftliche Lagerordnung (Festlegung des verantwortlichen Lagerhalters, der Lagerbuchführung, der Sicherheitsmassnahmen, der Bestandskontrollen etc.)?	3	60%	3	Logistik	ERP-System
#8	Anlagevermögen: Wie ist die Kompetenzregelung bezüglich Investitionen (Antrag, Entscheid, Beschaffung) gestaltet?	5	15%	5	Finanzsystem/Logistik/ Management/Controlling	–
#9	Anlagevermögen: Wie sind die Zuständigkeiten bezüglich der Anlagenbuchhaltung geregelt?	3	40%	3	Finanzsystem	ERP-System
#10	Anlagevermögen: Einkauf und Verbindlichkeiten: Funktionstrennung: Ist der Wareneingang vom Einkauf getrennt?	3	15%	2	Einkauf/Logistik	ERP-System
#11	Einkauf und Verbindlichkeiten: Ist die ordnungsgemässe Zahlung (Gefahr der Doppelzahlung, Skonto, Anzahlungen, Gegenforderungen) sichergestellt?	4	40%	**3**	Rechnungswesen	ERP-System
#12	Personalwesen/Personalaufwand: Wie stellt die Funktionstrennung selbstständige Kontrollen sicher?	5	50%	5	Human Resources	HR-System

Grafik 1: Risikoidentifikation und Bewertung