05.16

11. Jahrgang
Oktober 2016
Seiten 193–240

ZRFC

Risk, Fraud & Compliance

www.ZRFCdigital.de

Prävention und Aufdeckung durch Compliance-Organisationen

ERICH SCHMIDT VERLAG

In Kooperation mit
DICO
Deutsches Institut für Compliance

64683

IT-Compliance durch Nutzungsanalyse

Verwendung der Nutzungsanalyse als kompensierende Kontrolle für Funktionstrennungskonflikte

Karl Ulber*

Karl Ulber

Die belegbasierte Nutzungsanalyse stellt einen toolbasierten methodischen Ansatz zur Identifikation kritischer Buchungsvorgänge dar, die unter Verwendung sensitiver Berechtigungen und deren Kombination in Form von Funktionstrennungskonflikten durch Benutzer im IT-System erzeugt wurden. Die Nutzungsanalyse kann somit maßgeblich als kompensierende Kontrolle für Funktionstrennungskonflikte im Rahmen der IT-Compliance eingesetzt werden.

1 Ausgangssituation

Laut einer aktuellen Studie von PwC sind ca. 57 Prozent aller befragten Unternehmen von klassischer Wirtschaftskriminalität betroffen.[1] Darunter fallen unter anderem der Diebstahl vertraulicher Kunden- und Unternehmensdaten als auch die Manipulation von Konto- und Finanzdaten. Ein wesentliches Einfallstor für Wirtschaftskriminalität im Unternehmen kann dabei eine unangemessene Adressierung der IT-Sicherheit und deren Forderung nach Einhaltung des Minimalprinzips bei der Berechtigungsvergabe sein. Konkret bedeutet dies, dass Mitarbeiter Berechtigungen in rechnungslegungsrelevanten IT-Systemen erhalten, die nicht für die Ausführung ihrer Tätigkeit erforderlich sind. Dabei können die Ursachen für die Verletzungen des Minimalprinzips verschiedenartig sein: Angefangen mit der Zuordnung zu weitreichender Rechte bei der initialen Versorgung, über den fehlenden Entzug von Altberechtigungen bei Personalbereichswechseln bis hin zum fehlenden Entzug oder Befristung der Benutzer und Berechtigungen bei vorübergehender Inaktivität oder beim Verlassen des Unternehmens. Neben der Verletzung des Minimalprinzips ergeben sich hieraus als Kollateralschaden noch Berechtigungskombinationen, die gegen die Funktionstrennungsprinzipien verstoßen (z. B. Berechtigungen die zur Erfassung fiktiver Bestellungen in Kombination mit der Freigabe einer korrespondierenden Eingangsrechnung zur Zahlung befähigen).

Unternehmen können diese Risiken vermeiden oder zumindest verringern, indem sogenannte toolgestützte Potenzialanalysen durchgeführt werden. Dabei wird ermittelt, welche Mitarbeiter IT-Berechtigungen für die Ausführung sensitiver (Einzel-) Funktionen sowie für die Ausführung von Kombinationen sensitiver Funktionen (Funktionstrennungskonflikte) besitzen. Die Adressaten dieser Auswertungen (u. a. insbesondere die Interne Revision) erhalten dadurch zwar Aussagen über das mögliche Risikopotenzial, nicht jedoch darüber, ob die ermittelten Benutzer tatsächlich dieses Potenzial in Form der Erfassung von Transaktions- oder Stammdaten genutzt/realisiert haben (z. B. durch Buchung einer Bestellung und Eingangsrechnung).

Die Nutzungsanalyse greift nun genau diesen fehlenden Aspekt der Potenzialanalyse auf, indem analysiert wird, welche Mitarbeiter tatsächlich ihre Berechtigungen für die Ausführung von sensitiven Funktionen (engl.: SA – Sensitive Authorization) genutzt haben. Dabei werden innerhalb der IT-Lösungen die automatisch mitgeführten Protokoll-/Log-Daten für transaktionale, sensitive Geschäftsvorgänge ausgelesen und aufbereitet. Durch geschickte Verknüpfung der Log-Daten kann so ermittelt werden, welche Benutzer welche Funktionen für welche Organisationseinheiten ausgeführt haben und in Verknüpfung mehrerer Funktionen, welche Funktionstrennungskombinationen ausgeführt wurden. Die Interne Revision kann somit ergänzend zur Be-

* Karl Ulber ist Manager im Bereich Risk Assurance Solutions der PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft am Standort Leipzig und spezialisiert auf das Thema Identity-, Access- und Governance Management, Kontakt: Karl.Ulber@de.pwc.com.

1 Vgl. PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft & Martin-Luther-Universität Halle-Wittenberg (Hrsg.): Wirtschaftskriminalität in der analogen und der digitalen Wirtschaft 2016, Halle-Wittenberg 2016, S. 3, abrufbar unter http://www.pwc.de/wirtschaftskriminalität (Stand 07.06.2016).

trachtung der reinen Potenzialbetrachtung auch das Nutzungsrisiko in die Beurteilung mit einbeziehen und ihre Kontrollen auf die durch die Nutzungsanalyse ermittelten Belege fokussieren.

Der Artikel beschreibt einen methodischen Ansatz zur Entwicklung und zum Einsatz der toolbasierten Nutzungsanalyse. Um den Artikel praxisnah zu gestalten, sind einige Begrifflichkeiten aus dem SAP-Kontext bei der Erläuterung von Beispielen genannt. Der methodische Ansatz ist dabei aber nicht zwingend auf SAP-Systeme begrenzt.

2 Anwendungsfälle Nutzungsanalyse

2.1 Kompensierende Kontrollen im IKS

Die Vergabe und Nutzung von Berechtigungen sollte stets unter Beachtung der Vermeidung von Funktionstrennungskonflikten erfolgen. Die Basis dieser Anforderung stellt unter anderem ein dokumentiertes Regelwerk über sensitive Funktionen und deren Kombination in Funktionstrennungsregeln dar. Die Einhaltung solch eines Regelwerks kann dabei über Prozesskontrollen (z. B. durch ein Vier-Augen-Prinzip) oder nachgelagerte Kontrollen (z. B. durch eine nachgelagerte Einzelbelegprüfung) erfolgen. Verantwortlich für die Durchführung der Kontrollen ist in der Regel der Dateneigner, in dessen Fachbereich die sensitive Funktion angewandt wurde (Der Einkaufsleiter z. B. ist für die Überprüfung der erzeugten Bestellungen verantwortlich).

In Abhängigkeit der Unternehmensgröße bzw. des organisatorischen Aufbaus des Unternehmens können Funktionstrennungskonflikte jedoch durchaus in einigen Tätigkeitsbereichen für ausgewählte Benutzer (meist Keyuser) gewollt sein. Unabhängig davon, ob die Funktionstrennungskonflikte gewollt oder ungewollt sind, sind diese durch entsprechende Kontrollen zu adressieren. Da Prozesskontrollen mit einem hohen organisatorischen und personellen Aufwand verbunden sind, kann die Nutzungsanalyse an dieser Stelle zum Einsatz kommen. Mithilfe der Nutzungsanalyse kann der Dateneigner gezielt Belege für die nachgelagerte Prüfung identifizieren, die unter Anwendung von sensitiven Funktionen/Funktionstrennungskonflikten erzeugt wurden. Fokus der Belegprüfung sollte dabei auf Belegen von Mitarbeitern liegen, welche nicht dem Fachbereich entsprechen (z. B. wenn ein Mitarbeiter aus der Finanzbuchhaltung eine Bestellung erzeugt). Anstatt wahllos eine Stichprobe von Belegen aus dem Buchungsstoff einer Periode heraus zu greifen und „die Nadel im Heuhaufen zu suchen", kann mit der Nutzungsanalyse somit gezielt nach sensitivem Buchungsstoff gesucht werden.

2.2 Rezertifizierung von Berechtigungszuordnungen

Vielen Unternehmen mangelt es an Keyusern bzw. an Netzwerken von Keyusern, welche in der Lage sind, aus der Tätigkeit eines Benutzers dessen konkreten Bedarf an Berechtigungen in Form von Rollen abzuleiten. Als Folge werden Benutzern durch deren zuständige Manager in der Regel mehr oder sogar falsche Berechtigungen zugeordnet als tatsächlich notwendig. Dies wiederum stellt eine Verletzung des Minimalprinzips dar und kann zu ungewollten Funktionstrennungskonflikten führen.

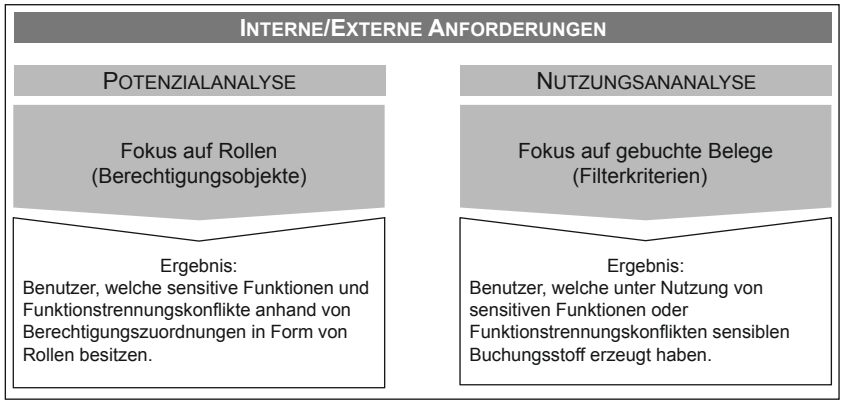

Abbildung 1: Gegenüberstellung Potenzial- versus Nutzungsanalyse

Diesen Mangel versuchen Unternehmen meist zu kompensieren, indem mindestens einmal jährlich die Benutzern zugeordneten Berechtigungen durch deren Manager auf Aktualität und Notwendigkeit geprüft und rezertifiziert werden. Insbesondere Berechtigungen, die nur kurzfristig z. B. aufgrund von Vertretungsaufgaben Mitarbeitern zugeordnet wurden (jedoch nach dem Wegfall der Vertretungsfunktion nicht wieder entzogen wurden), sollen dadurch aufgespürt und bereinigt werden.

Bei der Berechtigungsvergabe muss das Minimalprinzip berücksichtigt werden.

Für den Vorgesetzten kann diese Rezertifizierung durchaus eine komplexe und zeitaufwendige Kontrolle in Abhängigkeit des technischen Verständnisses des Vorgesetzten für Berechtigungen sowie der Anzahl der zu rezertifizierenden Mitarbeiter darstellen. Zudem scheuen sich oft auch Vorgesetzte, eine Berechtigung, die sie konkret nicht beurteilen können, zu entziehen, um hierdurch keinen Produktionsstillstand oder Arbeitsunfähigkeit des Benutzers zu provozieren.

Die Nutzungsanalyse kann dabei den Rezertifizierungsprozess maßgeblich optimieren, da in der Regel bei dem Rezertifizierungsprozess vor allem die Ergebnisse aus der Potenzialanalyse dem zuständigen Manager zur Überprüfung bereitgestellt werden. Werden nun die Ergebnisse aus der Potenzialanalyse (welcher Benutzer hat welche [sensitive] Berechtigung zugeordnet) mit den Ergebnissen der Nutzungsanalyse (welcher Benutzer hat welche [sensitiven] Funktionen im ERP-System tatsächlich durchgeführt) kombiniert, erhält der zuständige Manager eine klare Indikation für einen Berechtigungsentzug-Antrag über nicht genutzte Berechtigungen im Auswertungszeitraum. Als Ergebnis wird die Arbeit der zuständigen Manager im Rezertifizie-

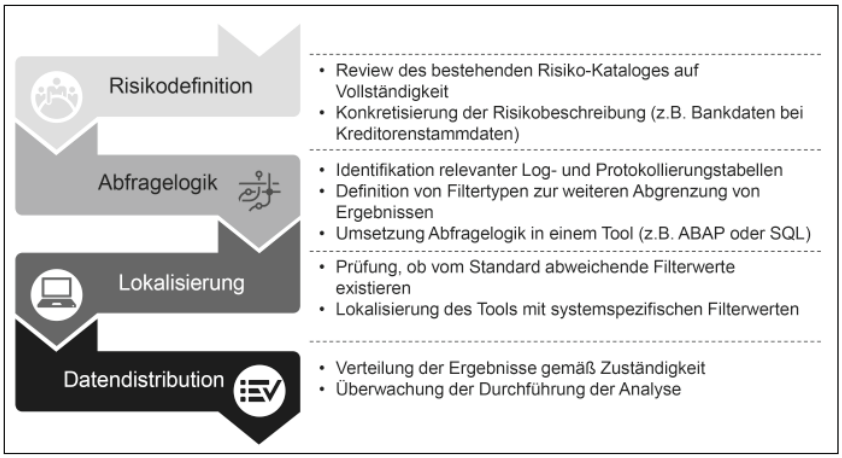

Abbildung 2: Projektschritte der Nutzungsanalyse

Typ	ID	Funktion	Risiko	Beschreibung
SA	SA_1	Debitoren-Stammdaten pflegen	Hoch	Ein Mitarbeiter könnte in einem Debitor eine falsche Bankverbindung oder andere zahlungsrelevante Felder pflegen. Eine falsche Bankverbindung könnte zu einer Überweisung auf ein falsches Konto oder einem fehlerhaften Einzug beim Debitor führen. Der Benutzer könnte dadurch einen Dritten oder sich selbst bereichern.
SA	SA_2	Zahllauf durchführen	Hoch	Benutzer könnte fiktive Zahlungen veranlassen. Aufgrund des unberechtigten Zahlungsabflusses würde eine unzutreffende Darstellung in Bilanz und GuV entstehen. Benutzer könnten sich oder Dritten einen finanziellen Vorteil verschaffen.
SoD	SoD_1	Debitoren-Stammdaten pflegen & Zahllauf durchführen	Hoch	Benutzer könnte für einen Debitor mit einer anstehenden Gutschriftsüberweisung die Bankdaten ändern und die Gutschrift zur Auszahlung bringen. Der Benutzer könnte dadurch einen Dritten oder sich selbst bereichern.

Abbildung 3: Beispiel Risikokatalog

rungsprozess erheblich vereinfacht und die zugeordneten Berechtigungen zunehmend den tatsächlichen Tätigkeiten der Mitarbeiter und damit dem Minimalprinzip angenähert.

2.3 Identifikation von Prozessabweichungen

In Abhängigkeit der Größe und der Komplexität der IT-Landschaft können Prozessketten verteilt über mehrere ERP-Systeme verlaufen (z.B. auf System A werden Bestellungen gebucht, auf System B werden die Eingangsrechnungen erfasst und auf System C wird schließlich der Zahllauf durchgeführt). Handelt es sich zudem um ein Unternehmen mit unterschiedlichen Geschäftsbereichen, die nicht auf einem gemeinsamen Prozessrahmenwerk aufbauen und von denen jeder Geschäftsbereich eigene Standards entwickelt hat, kann dies aufgrund einer fehlenden Dokumentation zu einer intransparenten Prozesslandschaft führen.

Gewollte oder ungewollte Funktionstrennungskonflikte sind durch kompensierende Kontrollen zu mitigieren.

Licht ins Dunkel kann hier die Nutzungsanalyse bringen. Pro installiertem ERP-System wird geprüft, welche Funktion für welche Gesellschaft (z.B. abgrenzbar anhand des Buchungskreises einer Gesellschaft) auf dem jeweiligen System ausgeführt wird. Werden nun die Ergebnisse aller Systeme konsolidiert und nach Gesellschaft aufbereitet, ergibt sich ein klares Bild darüber, welche Gesellschaft welche Funktion auf welchem System ausführt.

Neben dem Aspekt der Transparenz können anhand der Prozesslandschaft auch prozessuale Abweichungen erkannt werden. Sofern ein zentrales Prozessrahmenwerk existiert und dieses vorschreibt, welches System wie zu nutzen ist, kann deren Einhaltung überprüft werden. Sind z.B. neben System A auch Bestellungen auf System B gebucht worden, handelt es sich um eine Abweichung von den zentralen Vorgaben, die zu hinterfragen ist.

2.4 Benchmarking SA/SoD-Regelwerke

Grundlage für die Nutzungsanalyse ist ein Regelwerk für sensitive Funktionen und Funktionstrennungsregeln, welches die prozessualen Risiken des Unternehmens bestmöglich beschreiben und adressieren soll. Sofern kein jährlicher Rezertifizierungsprozess für die Überprüfung des Regelwerks auf Aktualität und Angemessenheit etabliert ist, können somit ggf. im Unternehmen bestehende Risiken nicht korrekt adressiert werden. Ein Projekt zur Einführung eines Tools wie die belegbasierte Nutzungsanalyse liefert dabei eine gute Gelegenheit solche Risikokataloge zu überprüfen. Da entsprechende Projekte zudem meist von externen Beratern begleitet werden, können diese ihr Branchen- und Prozess-Know-how mit einbringen und somit wertvolle Hinweise für die Optimierung des Regelwerkes beisteuern. Dabei kann unter anderem geprüft werden, ob das bereits vorhandene Regelwerk der Best Practice von vergleichbaren Unternehmen (in Abhängigkeit der Größe und Branche) entspricht.

3 Methodik

Ein Projekt zum Design bis hin zur Implementierung eines Nutzungsanalyse-Tools lässt sich typischerweise in vier Prozessschritte unterteilen. Je nach vorhandenem Prozess- und Programmierungs-Know-how empfiehlt es sich, Unterstützung durch einen externen Berater und/oder Programmierer temporär einzukaufen.

3.1 Risikodefinition/-beschreibung

Wesentlicher Erfolgsfaktor für die Nutzungsanalyse ist eine konkrete Risikodefinition und -beschreibung, die mithilfe der Beleganalyse geprüft werden soll. Werden die Risiken zu generisch beschrieben, können Belege als Treffer identifiziert werden, die als unkritisch anzusehen sind (False Positive). Als Beispiele wären die Pflege von Kreditorenstammdaten und die Durchführung von Zahlläufen zu diesen Kreditoren zu nennen. Ohne Konkretisierung des Risikos der Pflege der Bankverbindungsdaten als kritisches Element innerhalb der Kreditorenstammdaten, würden u.a. auch Belegtreffer angezeigt werden, bei denen z.B. lediglich die Telefonnummer des Kreditors gepflegt wurde. Die Erarbeitung einer Risiko-

beschreibung sollte dabei immer unter Einbindung von Fachbereichsvertretern (Keyusern) in Form von Workshops erfolgen, da diese noch zusätzliche Hinweise ggf. zu Prozessbesonderheiten geben können.

Die Ergebnisse der Risikobeschreibungs-Workshops sollten zum Abschluss dieser Phase in einem Lastenheft festgehalten werden. Das Lastenheft dient als Ausgangsbasis für die technische Umsetzung der Beleganalyse.

ID	Funktion	Filtertyp	Standard	Lokalisierung
SA_1	Bestellung pflegen	Belegtyp	F – Bestellung K – Kontrakt	
SA_2	Gutschriftsanforderung buchen	Auftragsart	G2 – Gutschrifts-anforderung	ZG2 – Gutschrift Neu
		Kontoart	D – Debitoren	

Abbildung 4: Beispiel einer Abfragelogik für SAP

3.2 Entwicklung Abfragelogik & technische Umsetzung

Nachdem die Risiken ausreichend detailliert beschrieben wurden, ist für die Risiken jeweils eine Abfragelogik zur Identifizierung der relevanten Vorgänge in den IT-Systemen zu entwickeln. Die wichtigsten Arbeitsergebnisse dieser Projektphase sind die Identifizierung sowohl der relevanten Tabellen, in denen die zu den Risiken korrespondierenden Belege abgespeichert werden, als auch die Identifizierung von Filtertypen, um die Belege innerhalb der Zieltabelle weiter einzugrenzen. Sind zum Beispiel bei Vertriebsaufträgen nur Gutschriftsanforderungen und keine Lieferaufträge von Relevanz, kann dies über den Filtertyp Auftragsart gesteuert werden. Sollen neben sensitiven Funktionen auch Funktionstrennungskonflikte abgeprüft werden, sind pro Einzelfunktion die relevanten Felder zur Verknüpfung der Belege untereinander zu identifizieren (z. B. können Eingangsrechnungen und Zahlläufe über die Felder Benutzer und Belegnummer verknüpft werden).

Als Hilfsmittel zur Identifizierung der Zieltabellen pro Funktion kann einerseits auf die Protokollierungsfunktion des IT-Systems als auch auf gezielt erzeugte Testbelege pro Funktion zurückgegriffen werden. Im SAP-Kontext werden z. B. Änderungen an Bewegungsdaten wie die Pflege von Bestellungen in der Änderungstabelle (Tabelle CDHDR) erfasst, während Änderungen an Konfigurationsdaten wie das Öffnen und Schließen von Buchungsperioden anhand der Systemprotokollierung (Tabelle DBTAGLOG) nachvollzogen werden können.

Sind die relevanten Tabellen und Filtertypen identifiziert, sind diese schließlich in einem Tool umzusetzen. Nach Fertigstellung der Entwicklung sollten in Zusammenarbeit mit dem Fachbereich sowohl False Positive Tests als auch False Negative Tests erfolgen. Bei den False Positive Tests wird mit der Nutzungsanalyse der bereits vorhandene Buchungsstoff analysiert und geprüft, ob dieser der Erwartungshaltung entspricht. Bei den False Negative Tests wird hingegen neuer Testbuchungsstoff generiert, der durch das Tool zutreffend identifiziert werden muss.

3.3 Lokalisierung

Ist das Beleganalyse-Tool auf der produktiven Instanz des IT-Systems einsatzbereit, muss das Tool noch auf die systemspezifischen Prozessgegebenheiten lokalisiert werden. Werden im SAP-Kontext zum Beispiel Gutschriftsanforderungen im SAP Standard per Auftragsart G2 erfasst, muss geprüft werden, ob ggf. systemspezifische Auftragsarten wie ZG2 für die Erzeugung von Gutschriftsanforderungen verwendet werden. In solchen Fällen sind die systemspezifischen Werte in die lokale Anpassung der Nutzungsanalyse aufzunehmen. Somit wird sichergestellt, dass keine relevanten Belege bei der Ermittlung der Belegtreffer ausgeschlossen werden.

Sofern das Tool konfiguriert wurde, kann die Datenbeschaffung gestartet werden. Dabei sind möglichst Abgrenzungskriterien wie Auswertungszeitraum und Buchungskreise vor dem Programmstart zu definieren.

3.4 Datendistribution und -monitoring

Liegen die Belegtreffer vor, sind diese an die entsprechenden Adressaten zur Validierung zu verteilen. Wird die Nutzungsanalyse zum Beispiel im Rahmen des IKS als kompensierende Kontrolle verwendet, sind je nach analysierten Funktionsbereichen (Einkauf, Finanzen, etc.) sowie der analysierten Legal-Einheiten (Buchungskreis 1, Buchungskreis 2, etc.) entsprechende Adressaten zu bestimmen. Verantwortlich für die Kontrolldurchführung sollte dabei immer der Eigner der Daten sein, welche durch die sensitive Funktion verändert worden sind. Wurde zum Beispiel analysiert, welcher Benutzer Zahlläufe für Buchungskreis 1 durchgeführt hat, sollte der Rechnungswesen-Leiter des Buchungskreises 1 für die Kontrolle verantwortlich sein.

Bei der Nutzungsanalyse sind systemspezifische Prozessgegebenheiten zu berücksichtigen.

Sind die Ergebnisse verteilt, sollte deren Prüfung durch den zuständigen Adressaten von einer zentralen Instanz aus überwacht werden. Ebenso sollte die Dokumentation der Prüfungshandlungen an einer zentralen Stelle (Abteilungslaufwerk, Sharepoint, Workflow etc.) abgelegt werden. Dabei unterstützen kann auch das Nutzungsanalyse-Tool, in dem pro Trefferzeile hinterlegt werden kann, wer wann mit welchem Ergebnis die Prüfung durchgeführt hat.

4 Erfahrungen aus der Praxis

4.1 Involvierung Betriebsrat und Datenschutz

In Projekten, die die Analyse von Buchungsstoff zum Ziel haben und dabei unter anderem ermitteln, welcher Mitarbeiter wann Belege erzeugt hat, stellt das

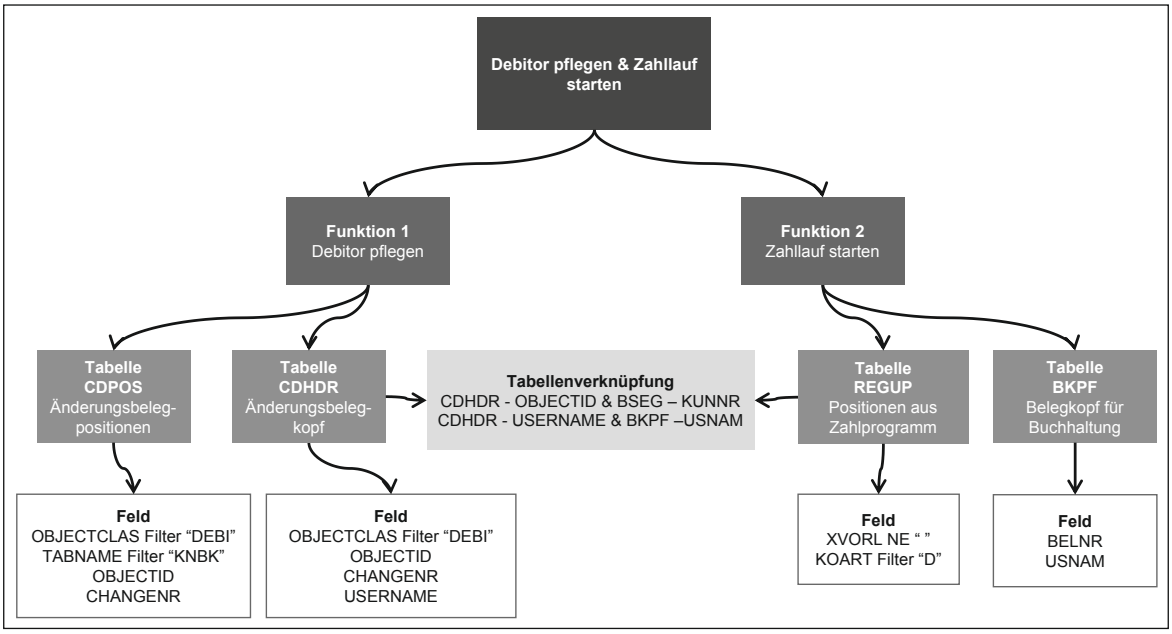

Abbildung 5: Beispiel Lokalisierungsübersicht

Thema Datenschutz und Leistungsüberwachung ein nicht zu vernachlässigender Projektaspekt dar. Daher ist es ratsam, gleich zu Projektbeginn den Betriebsrat und den Datenschutzbeauftragten zu involvieren und diesen über den geplanten Einsatzzweck der Software – die Identifikation von kritischem Buchungsstoff – zu unterrichten.

Ein wesentlicher Erfolgsfaktor für die Nutzungsanalyse stellt die Einbindung von Fachbereichs-Keyusern sowie des Betriebsrates dar.

In der bisherigen Praxis hat es sich unter anderem als nützlich erwiesen, die Ausgabe der kritischen Belege flexibel über sogenannte Konsolidierungsstufen zu gestalten, anstatt die Grundgesamtheit an gefundenen kritischen Belegen auszugeben. Demnach wird z.B. auf einer hohen Konsolidierungsstufe nur ausgegeben, wie viele Mitarbeiter insgesamt kritische Belege erzeugt haben, ohne im Detail die konkreten Namen aufzuführen.

Alternativ kann das Thema der Leistungsüberwachung auch damit umgegangen werden, indem nur Stichproben durch das Tool bereitgestellt werden, anstatt die Grundgesamtheit an Belegtreffern pro Benutzer aufzuführen. Da die Revision in der Regel stichprobenorientiert prüft, kann das Programm im Hintergrund zwar die Grundgesamtheit aller kritischen Belege ermitteln, die Ausgabe wird jedoch nur auf eine Stichprobengröße beschränkt. Somit können keine Rückschlüsse auf die vollständige Anzahl der gebuchten Belege eines Mitarbeiters gezogen werden.

Das Programm wird zudem nicht der Allgemeinheit zur Verfügung gestellt, sondern nur einem berechtigten Adressatenkreis. Somit kann eine missbräuchliche Nutzung über Berechtigungen eingeschränkt werden.

4.2 Aufbau Expertennetzwerk

Der wesentliche Erfolgsfaktor für die Vermeidung von False Positive und False Negative Belegtreffern ist eine sauber durchgeführte Lokalisierung des Programms unter Berücksichtigung der systemspezifischen Eigenheiten. Werden z.B. Debitorengutschriften nicht wie im Standard über die Belegart DG gebucht, sondern über eine systemspezifische Belegart wie ZDG, ist dies entsprechend in der Lokalisierung zu berücksichtigen.

Daher werden von Unternehmensseite Experten benötigt, die sich sowohl in den Prozessen des Unternehmens als auch in deren technischen Umsetzungen in den IT-Systemen auskennen. In der Regel sind solche Keyuser nicht offiziell als solche im Unternehmen nominiert. Daher sollte bereits zu Beginn des Projektes versucht werden, solche Keyuser zu identifizieren und in das Projekt aktiv einzubinden, da externe Berater zwar Vorschläge für die Lokalisierung im Standard mitbringen können, ggf. relevanter Buchungsstoff aber durch eine unvollständige Lokalisierung aufgrund des fehlenden Know-hows von Keyusern nicht berücksichtigt wird.

4.3 Flexible Gestaltung der Abfragelogik

Risiken ändern sich mit der Zeit. Es kommen neue Risiken hinzu oder bestehende ändern sich in ihrer Ausrichtung. Genauso wie sich Risikokataloge ändern, muss sich somit auch die Nutzungsanalyse an die geänderten Risiken anpassen, was mitunter in der Vorhaltung einer ständigen Programmierer-Ressource enden kann, sofern das Nutzungsanalyse-Tool nicht eine gewisse Flexibilität mitbringt.

Flexibilität kann vor allem durch die Lokalisierung erreicht werden, indem Filtertypen und deren Filterwerte (wie Auftragsart G2) nicht fest kodiert in den Quellcode geschrieben werden, sondern als Parameter innerhalb des Tools konfiguriert werden können. Somit können zumindest prozessuale Unterschiede zwischen verschiedenen IT-Systemen leicht abgedeckt werden.

Sind hingegen neue Risiken aufzunehmen, empfiehlt es sich, das Tool von Anfang an so zu designen, dass flexibel bestehende oder neue Risiken samt relevanten Tabellen angepasst und ergänzt werden können. Somit wird eine Flexibilität erreicht, ohne ständig Programmierer mit den Anpassungen beauftragen zu müssen.

5 Fazit und Ausblick

Im Rahmen der IT-Compliance sind Unternehmen mit verschiedenen Anforderungen, wie der Einhaltung des Minimalprinzips sowie der Funktionstrennung bei der Vergabe und Nutzung von Berechtigungen für ihre IT-Systeme konfrontiert. Die Kontrolle der Einhaltung dieser Anforderungen erweist sich in der Regel als herausfordernd, da für Prozesskontrollen Zeit und Mittel fehlen bzw. durch nachgelagerten Kontrollen anhand der Potenzialanalyse nur eine Risikoindikation gegeben wird, anstatt eine Aussage darüber zu treffen, ob das Risiko tatsächlich realisiert wurde.

Die belegbasierte Nutzungsanalyse erweist sich dabei als ideale Ergänzung zur Potenzialanalyse, indem diese gezielt kritischen Buchungsstoff, der unter Verwendung von sensitiven Berechtigungen bzw. Funktionstrennungskonflikten erzeugt wurde, aufzeigt. Die Nutzungsanalyse kann dabei innerhalb von nur vier Prozessschritten im Unternehmen etabliert und in das Interne Kontrollsystem des Unternehmens integriert werden.

Die Nutzungsanalyse unterstützt bei der Einhaltung von IT-Compliance-Anforderungen.