Sven Petermann, Aleksandra Sowa

Governance Risk Compliance im SAP-Umfeld der Banken

Die Implementierung spezifischer Zugriffskontrollen ist für die Einhaltung geltender Gesetze bezüglich einer verlässlichen Finanzberichterstattung von erheblicher Bedeutung. Die Unternehmen müssen u.a. jederzeit den Nachweis erbringen können, dass nur berechtigte Personen Zugriff auf die geschäftskritischen Daten haben. Ohne unternehmensspezifisch ausgestaltete und regelmäßig beurteilte Zugriffskontrollen kann die Verlässlichkeit der generierten rechnungslegungsrelevanten Daten nicht ausreichend sichergestellt werden. Doch viele der Unternehmen betrachten die Compliance und die damit verbundenen Vorschriften als Kostentreiber. Dagegen kann eine effiziente und effektive Umsetzung der Zugriffskontrollen, beispielsweise durch den Einsatz eines Governance-Risk-Compliance- (GRC-) Tools, dem Unternehmen einen komparativen Wettbewerbsvorteil verschaffen.

Inhaltsübersicht

1 IT-Compliance – was bedeutet das eigentlich?

Auf europäische Unternehmen sind durch die 8. EU-Richtlinie, die seit Juni 2008 für alle Kapitalgesellschaften bindend ist, viele neue Herausforderungen bezüglich Compliance und Risikomanagement zugekommen. In Deutschland dient das Gesetz zur Modernisierung des Bilanzrechts (Bilanzrechtsmodernisierungsgesetz, BilMoG) der Umsetzung der EU-Richtlinie[1] und zugleich der Reform des Bilanzrechts. Dadurch soll u.a. die Aussagekraft der handelsrechtlichen Jahresabschlüsse verbessert werden. Wie davor SOX für die an der US-Börse notierten Unternehmen, so unterstreichen die aktuellen regulatorischen Rahmenbedingungen die Notwendigkeit, Kontrollen in Prozessen zu definieren und diese konsistent umzusetzen.

Gesetze und Normen verlangen von den Unternehmen mehr Transparenz im Umgang mit Daten. Unternehmen stehen nunmehr in der Pflicht, sämtliche Geschäftsprozesse ständig zu analysieren und zu dokumentieren. Die Ordnungsmäßigkeit und Wirksamkeit des internen Kontrollsystems (IKS) und des Risikomanagements im Allgemeinen muss in Audits geprüft und beurteilt werden. Zudem müssen die Unternehmen jederzeit den Nachweis erbringen können, dass nur berechtigte Personen Zugriff auf die geschäftskritischen Daten haben und diese nicht manipuliert werden können.

1. Konkret sind hier die sog. Abschlussprüferrichtlinie (Richtlinie 2006/43/EG in Ergänzung durch die Richtlinie 2008/30/EG) und die sog. Abänderungsrichtlinie (Richtlinie 2006/46/EG) gemeint.

Im Rahmen des Risikomanagements spielen daher das Zugriffsberechtigungsmanagement sowie die Zugriffskontrollen (Access Controls) eine zentrale Rolle. Dies sowohl im Hinblick auf die Compliance mit den Vorgaben über Datenspeicherung und Archivierung – denn im Zweifelsfall sollen die Daten vor absichtlicher oder versehentlicher Manipulation oder Löschung geschützt werden – als auch bezüglich der u.a. im Transaktionsumfeld geforderten Funktionstrennung (sog. Segregation of Duties).

2 Die Chance: Wettbewerbsvorteil durch standardisierte Compliance-Prüfung

Viele der gesetzlichen Auflagen geben lediglich das Grundgerüst für die Compliance vor und legen nicht fest, wie die Lösungen im Detail aussehen sollen. Die in den Unternehmen umgesetzten Maßnahmen ermöglichen es in den meisten Fällen, die entsprechenden Audits durch die externen Prüfer zu bestehen. Doch viele der betroffenen Unternehmen betrachten die Compliance als Kostentreiber, als eine Verpflichtung, die nur mit exorbitanten Kosten umsetzbar ist und keinen Mehrwert für das Unternehmen im Allgemeinen hat. Dagegen können eine effiziente und effektive Umsetzung der IT-Kontrollen und nachhaltige Compliance dem Unternehmen einen komparativen Wettbewerbsvorteil verschaffen.

Die GRC-Tools sind ein Beispiel dafür, wie solche Wettbewerbsvorteile konkret realisiert werden können. Der Wettbewerbsvorteil lässt sich hier auf zwei Ebenen bewerkstelligen: (1) durch Realisierung von Kostenvorteilen (Savings) und (2) durch Erzielen eines »Reputationsvorsprungs« gegenüber den Wettbewerbern.

2.1 Savings: Repetitives Lernen durch Automatisierung

Als einer der wichtigsten Gründe für die hohen Kosten der Compliance – und folglich der Compliance-Prüfungen – wird eine fehlende Standardisierung der Geschäftsprozesse für die kritischen, rechnungslegungsrelevanten Systeme genannt. Schätzungsweise 70 Prozent der von Auditoren identifizierten Mängel sind auf die Nichtverfügbarkeit von standardisierten Prozessen zurückzuführen [Mehta 2009].

»There may be sufficient processes to get the right people involved with the right information at the right time ...«, stellt Barnier [Barnier 2009, S. 38] fest, »... but there may be too little automation, so that manual paperwork gets out of control.« Durch Standardisierung und Automatisierung der Compliance-Prozesse können folglich Einsparungen realisiert werden, da Aufwände für die Verwaltung von Benutzern und Berechtigungen größtmöglich minimiert und die Kosten einer manuellen Prüfung vermieden werden. Unter anderem kann das Nichtvorhandensein eines standardisierten Zugriffsverwaltungssystems zu manuellen und kostenintensiven Bereinigungen von Berechtigungen, Rollen und Benutzern führen.

Neben den kurzfristig realisierbaren Kostenersparnissen (vgl. dazu [Götz et al. 2008]) sind hier hauptsächlich die über mehrere Perioden realisierbaren Einsparungen durch repetitives Lernen gemeint [Kloock & Sabel 1992]. Voraussetzung, eine (kosten)effektive Standardisierung umsetzen zu können, ist eine Bewertung und Beurteilung aller geschäftskritischen Prozesse und Identifizierung des Verbesserungspotenzials – also die Durchführung eines sogenannten »Health Check« – bevor die Automatisierung umgesetzt und die entsprechenden Tools ausgewählt werden. Eine Daumenregel: Je besser ein Unternehmen bereits organisiert ist (je höher z.B. die »Maturity«), desto weniger Schwierigkeiten ergeben sich bei Standardisierung und Automatisierung der Compliance-Prozesse und ein umso höherer Mehrwert lässt sich durch diese Veränderungen realisieren.

2.2 Reputationsvorsprung

Eine – nach innen wie nach außen – wirksame Umsetzung der Compliance-Vorgaben hat eine

starke Signalwirkung und kann sich – gerade in den Rezessionszeiten – positiv auf das Unternehmensimage in der Branche und Öffentlichkeit auswirken. In zahlreichen Regelwerken (u.a. CobiT) wird Compliance als einer der durch Unternehmen erzeugten »Outputs« betrachtet und wirkt sich somit sowohl auf den Unternehmenswert als auch auf die Unternehmens-Performance aus.

Fälle von Korruption, Betrug oder Veruntreuung wirken sich negativ auf das Kundenvertrauen aus und können ggf. eine Abwanderung zum Wettbewerber verursachen. Das Gegenteil davon, d.h. eine Verankerung des Unternehmensbildes als »compliant«, sprich »clean« oder »ethisch«, hilft dem Unternehmen, sich von der Konkurrenz abzugrenzen, auf dem Markt zu positionieren und ggf. neue Kunden zu gewinnen. Dieser Hypothese liegt u.a. die Analyse von Pippa Norris zugrunde, die eine Entscheidung über einen Kauf oder Nichtkauf von Produkten bei einem bestimmten Unternehmen als eine moderne Ausdrucksform der politischen Partizipation identifiziert hat, sogenannte »consumer politics«, also »... buying or boycotting certain products for political or ethical reasons« [Norris 2003, S. 4]. So können Kunden im Rahmen ihrer individuellen Kaufentscheidungen entsprechend ihren politischen oder ethischen Überzeugungen die Unternehmen »bestrafen« oder »belohnen«. Diese »politischen« Entscheidungen sind für die betroffenen Unternehmen ertragswirksam.

3 Die Herausforderung: Zugriffsberechtigungen im Spannungsfeld der Compliance-Vorgaben

Das Hauptziel der Compliance-Vorschriften ist es, eine wahrheitsgetreue Berichterstattung zu garantieren. Das Problem dabei ist, dass es kein einzelnes Rahmenwerk gibt, das explizit vorgibt, was ein Unternehmen tun muss, um »compliant« zu sein. Vorgaben, die speziell für die Zugriffskontrollen relevant sind, sind Gegenstand zahlreicher externer Rahmenbedingungen.

3.1 Forderungen der Prüfer an Zugriffskontrollen

Die geltenden Gesetze, gesetzesähnliche Normen und Standards bilden eine Grundlage für die Ableitung konkreter Implementierungs- und Designhinweise für die Zugriffkontrollen. Die relevanten Vorschriften mit einer potenziellen Auswirkung auf das Design von Zugriffsberechtigungskontrollen sind u.a. die folgenden:

- Aktiengesetz (AktG) – § 91 Abs. 2,
- Bundesdatenschutzgesetz (BDSG) – § 9 Technische und organisatorische Maßnahmen bzw. Anlage zu § 9 Satz 1 BDSG (sog. »8 Gebote des Datenschutzes«),
- Grundsätze Ordnungsmäßiger Buchführungssysteme (GoBS) – Tz. 5 Datensicherheit,
- Kreditwesengesetz (KWG) – § 25 (gilt für Kreditinstitute),
- Mindestanforderungen an das Risikomanagement (MaRisk) der BaFin – Ziffer AT 7.2 (gilt für Kreditinstitute).

Gesetze und Normen verweisen oft auf die »gängigen Standards«, wenn es um die Konkretisierung der Vorgaben bezüglich Zugriffskontrollen geht. Hierzu zählen hauptsächlich:

- ISO 27002 (bisher ISO 17799:2005) »Information technology – Code of practice for information security management« – insbesondere Tz. A.11 Access Control (Zertifizierung möglich) sowie
- Standard des BSI 100-2 und das Grundschutzhandbuch des BSI (ISO-27001-Zertifizierung auf der Basis von IT-Grundschutz möglich).

Ebenfalls können Frameworks wie Control Objectives for Information and related Technology (CobiT) oder IT Infrastructure Library (ITIL) hilfreich sein. Dabei werden bei der Entwicklung von CobiT die bestehenden o.g. Standards zum Thema Sicherheitsmanagement berücksichtigt.

Wertvolle Hinweise für die Prüfung der Zugriffskontrollen können den ausführlichen Leitfäden im Form von Standards des IDW (Instituts der Wirtschaftsprüfer) für die externen und internen Prüfer entnommen werden, z.B. IDW PS 330 und IDW RS FAIT1 für die Prüfung von IT-Systemen, falls rechnungslegungsrelevante Teile der IT-Systeme bei der Abschlussprüfung berücksichtigt werden sollen.

Die Existenz eines internen Kontrollsystems (IKS) sowie dessen Ordnungsmäßigkeit und Wirksamkeit sind Prüfungsgegenstand der externen (und internen) Auditoren bzw. Wirtschaftsprüfer. In vielen Branchen, wie z.B. bei den Kreditinstituten, ist die Einführung eines IKS den Unternehmen direkt vorgeschrieben (vgl. KWG und MaRisk). Bei den anderen wird die effektive und effiziente Umsetzung des IKS indirekt über den Prüfungsgegenstand des Audits angesprochen. In beiden Fällen besteht die Pflicht, die Ordnungsmäßigkeit und Wirksamkeit des IKS gegenüber sachverständigen Dritten nachweisen zu können.

Die Zugriffskontrollen sind ein integraler Bestandteil des Kontrollsystems. Einerseits dienen sie der Sicherstellung von rechnungslegungsrelevanten Daten (Finanzinformationen), die innerhalb von IT-Systemen und Applikationen erzeugt werden. Andererseits sind sie im Rahmen der Applikationskontrollen verankert, wo sie die vollständige, fehlerfreie, autorisierte und gültige Erfassung, Manipulation und Ausgabe von Transaktionen unterstützen (oft zusammen mit manuellen Kontrollen).

Die Implementierung spezifischer Zugriffskontrollen ist deshalb für die Einhaltung der bezüglich der Verarbeitung der Transaktionen und des Ausweises einer verlässlichen Finanzberichterstattung geltenden Gesetze von erheblicher Bedeutung. Ohne unternehmensspezifisch ausgestaltete und regelmäßig beurteilte Zugriffkontrollen kann die Verlässlichkeit der generierten rechnungslegungsrelevanten Daten nicht ausreichend sichergestellt werden. Zugriffskontrollen als eine der generellen IT-Kontrollen stehen oft im Fokus der Prüfungen durch die interne Revision. Sie können auch im Rahmen der Abschlussprüfung beurteilt werden. Externe Prüfer konzentrieren sich dagegen nur auf die Bestandteile des Zugriffskontrollsystems, die für die Rechnungslegung relevant sind (bei beiden Prüfungen gilt der risikoorientierte Prüfungsansatz).

3.2 Zugriffskontrollen in den Prüfungsstandards des Instituts der Wirtschaftsprüfer

Für die Prüfung der Ordnungsmäßigkeit und Wirksamkeit der o.g. Kontrollen liegen den Revisoren und externen Auditoren ausführliche Leitfäden zur Prüfung der Zugriffs- und Zugangsberechtigungen in Form von Standards des Instituts der Wirtschaftsprüfer (IDW) vor (IDW PS 330 und IDW RS FAIT1). Konkret liefern die IDW PS 330, Tz. 57 ff. sowie IDW RS FAIT1, Tz. 84 detaillierte Vorgaben, wann ein Zugriffsberechtigungssystem als ordnungsgemäß (»richtige Dinge tun«) und wirksam (»Dinge richtig tun«) zu beurteilen ist. So steht gemäß IDW PS 330 bei der Prüfung der Ordnungsmäßigkeit die Implementierung eines »organisatorischen Verfahrens« zur Beantragung, Genehmigung und Einrichtung von Benutzerberechtigungen (sog. Berechtigungsverwaltung) in IT-Systemen auf Betriebssystem- und Anwendungsebene im Fokus der Prüfer. Zugriffskontrollen können als angemessen beurteilt werden, wenn sie geeignet sind, sicherzustellen, dass die Berechtigungsverwaltung und die eingerichteten Systemrechte den Festlegungen im Sicherheitskonzept entsprechen und damit unbefugte Zugriffe auf Daten sowie Programmabläufe zur Veränderung von Daten ausgeschlossen sind [IDW 2002a].

Im IDW PS 330 wird also die Existenz eines Sicherheitskonzepts vorausgesetzt, das Vorgaben zu der Berechtigungsverwaltung (Einrichtung, Änderung, Entziehung, Sperrung von Berechtigungen) beinhaltet. Die Zugriffskontrollen müssen so ausgestaltet sein, dass die Identität

des Benutzers eindeutig feststellbar ist und nicht autorisierte Zugriffe abgewiesen werden. Den Mitarbeitern sollen also nur die Berechtigungen erteilt werden, die zur Wahrnehmung ihrer Aufgaben notwendig sind [IDW 2002b].

Ob die tatsächlichen Abläufe mit den definierten Verfahren und unternehmensinternen Vorgaben übereinstimmen, wird im Rahmen der Prüfung der Wirksamkeit bewertet, also bei der Prüfung, ob die Kontrollen effektiv umgesetzt wurden. Die Durchführung der folgenden Tests gehört zu den kritischen Aufgaben der internen Revision; externe Auditoren führen diese hauptsächlich nur dann durch, wenn sie sich von der effektiven Umsetzung der Zugriffskontrollen endgültig überzeugen möchten (d.h., wenn die Prüfung der Ordnungsmäßigkeit positiv ausgefallen ist).

Zum Ersten kann geprüft werden, ob die definierten Verfahren zur Benutzerverwaltung den tatsächlichen Abläufen zur Benutzeradministration und -pflege entsprechen. Zum Zweiten kann z.B. im Rahmen einer Stichprobenprüfung festgestellt werden, ob die eingerichteten Berechtigungen den beantragten Rechten und diese wiederum den tatsächlichen Aufgaben des Mitarbeiters entsprechen. Dabei findet die Umsetzung der Funktionstrennung (Segregation of Duties) sowie die Verwaltung sogenannter Superuser-Rechte besondere Berücksichtigung.

Werden im Rahmen der Prüfung Mängel bzw. Schwachstellen identifiziert, so kann die Wirksamkeit bzw. die Ordnungsmäßigkeit des Zugriffskontrollsystems nicht nachgewiesen werden und es müssen Maßnahmen getroffen werden, die zur Verbesserung der Sachverhalte und der Compliance mit den Vorschriften führen.

4 Die Lösung: Einsatz der GRC-Tools

Um die Kosten der Compliance-Prüfungen zu reduzieren und einen Mehrwert aus den Audits zu realisieren, greifen inzwischen zahlreiche Unternehmen auf die sogenannten Governance-Risk-Compliance-(GRC-)Tools zu. Auf Basis eines GRC-Frameworks, wie in Abbildung 1 dargestellt, kann ein Vorgehen für die Operationalisierung und Automatisierung der Compliance-Prozesse erarbeitet werden.

Mit externer Unterstützung kann dieses Vorgehen wirksam begleitet werden. So können Quick Checks zur Erhebung des Istzustandes, zur Identifikation der kritischen Prozesse und zur Identifikation von Handlungsbedarfen innerhalb des GRC-Frameworks durchgeführt und notwendige Funktionstrennungen definiert und in einer Potenzialstudie dargestellt werden. Ist bereits ein Auditprozess etabliert, können konkrete Maßnahmen zur Automatisierung und Optimierung durch Analyse und Review des Prozesses empfohlen und priorisiert werden. Das daraufhin gemeinsam mit dem Unternehmen verabschiedete GRC-Regelwerk kann abschließend mit den Wirtschaftsprüfern abgestimmt und zur Umsetzung freigegeben werden.

Die Phase der Umsetzung beinhaltet die Konzeption und Konfiguration der GRC-Tools und deren Integration in die Systemlandschaft. Potenzielle Risiken entlang der kritischen Prozesse werden minimiert, indem detektive und präventive Kontrollen etabliert werden. Regeln zur Identifikation von Funktionstrennungsverletzungen werden etabliert, um die Einhaltung der Funktionstrennung wirksam kontrollieren zu können.

Die detektiven Kontrollen prüfen, ob nicht zulässige Prozesse und Transaktionen durchgeführt wurden. Die dadurch entstandenen Compliance-Verstöße sollen durch entsprechende Maßnahmen korrigiert werden. Dies ist zum Beispiel dann notwendig, wenn ein und dieselbe Person Produkte bestellen und empfangen darf und für diese auch den Zahlvorgang auslösen darf. Durch präventive Kontrollen wird Risiken im Vorfeld proaktiv vorgebeugt, sodass diese erst gar nicht eintreten können. So kann z.B. durch entsprechende Kontrollen vor Ausführung einer Zahlung geprüft werden, ob der Zahlungsempfänger für den Empfang der Zahlung berechtigt ist oder auf einer sogenannten »schwarzen

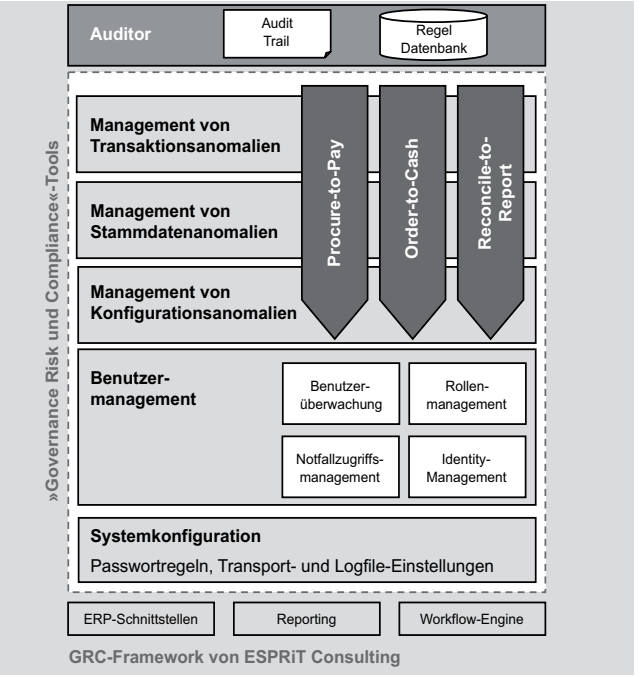

Abb. 1: GRC-Framework von ESPRiT Consulting

Liste« steht. Im letzteren Fall würde die Zahlung vom System nicht freigegeben werden.

Aufgabe des GRC-Tools ist es, diese Kontrollen in den angeschlossenen Businessapplikationen zu verankern sowie die Prozesse zur Steuerung und Kontrolle der Compliance effizient zu unterstützen.

Die Wettbewerbsvorteile, die durch Automatisierung und Standardisierung der Kontrollen im Rahmen des GRC-Tool-Einsatzes realisiert sowie durch den Reputationsvorsprung durch eine effektive Umsetzung der Compliance-Forderungen erzielt werden können, lassen sich am Beispiel der Zugriffskontrollen am deutlichsten visualisieren. Sowohl der Umfang der Kontrollen, ihre Gewichtung im internen Kontrollsystem als auch die Pflege verbundener Verwaltungsaufwände machen sie zu einem bedeutenden Kostenfaktor und können bei einer nachgewiesenen Unwirksamkeit (Beispiel von Jérôme Kerviel bei der französischen Bank Société Générale) zu einem enormen Reputationsverlust (neben den ertragswirksamen Verlusten) führen.

4.1 Die Vermeidung von Compliance-Risiken am Beispiel von SAP GRC Access Control

Die hohen Anforderungen an die Compliance-Prozesse lassen sich nur mit GRC-Tools erfüllen. In GRC-Tools werden Rollen und Regeln beschrieben, die aufgrund der unterschiedlichen Anforderungen des Business notwendig sind. GRC-Tools unterstützen automatisiert die effektive und unternehmensweite Kontrolle der Zugriffsberechtigungen auf Businessapplikationen durch autorisierte Nutzer. Diese Kontrollen gewährleisten das Einhalten einer klaren Funktionstrennung. SAP GRC Access Control ist durch Konnektoren mit Businessapplikationen wie SAP, Oracle oder PeopleSoft verbunden und bedient sich der dort existierenden Berechti-

gungsobjekte. Des Weiteren stellen GRC-Tools jederzeit einen Status bezüglich der Einhaltung der definierten Kontrollen zur Verfügung.

Funktionstrennungsrisiken bestehen, wenn ein Individuum die Möglichkeit hat, einen Geschäftsprozess von Anfang bis Ende ohne Beteiligung anderer Personen zu steuern. Schäden, die dadurch entstehen, werden im schlimmsten Fall nicht oder erst zu spät bemerkt. Eine Gefahr besteht zum Beispiel, wenn eine Person einen Lieferanten anlegt, eine Warenbestellung aufgibt und für diese Bestellung die Bezahlung auf das eigene Konto ausführt.

Durch Funktionstrennung, Verwendung von Einzelberechtigungen und Kontrolle der Berechtigungsvergabe werden Zugriffs- und Autorisierungsrisiken identifiziert und beseitigt. Dadurch wird verhindert, dass Kombinationen von Transaktionen ohne die Mitwirkung einer zweiten Person ausgeführt werden können. Die Funktionstrennung bleibt durch automatisierte Zugriffskontrollen und entsprechende Autorisierungsprozesse erhalten. Die Überprüfung der Rollendefinitionen und Etablierung eines Rollenmanagements kann ebenso unter Einsatz von SAP GRC Access Control erfolgen. Durch ein proaktives Risikomanagement werden Prozesse so überwacht, dass Risiken minimiert bzw. komplett vermieden werden können. SAP GRC Access Control ermöglicht ein zentralisiertes Rollenmanagement über alle Businessapplikationen (z.B. SAP, Oracle, PeopleSoft) hinweg.

Folgende Funktionalitäten werden durch SAP GRC Access Control bereitgestellt:

1. *Risikoanalyse und Bereinigung*
   SAP GRC Access Control vollzieht die Identifizierung, Überwachung und Reduzierung von Funktionstrennungsrisiken bzw. deren Bereinigung. Des Weiteren erfolgen eine automatisierte Analyse der Risiken und deren kontinuierliche Überwachung inklusive Alarmfunktion und Bereitstellung von Compliance-Berichten.

   SAP GRC Access Control bedient sich bei der Risikoprüfung der Echtzeitdaten, die ohne Unterbrechung aus den eingesetzten Systemen abgezogen werden. Dies ermöglicht die unverzügliche Identifizierung von Risiken und deren schnellstmögliche Bereinigung.
2. *Regel- und gesetzeskonforme Berechtigungsvergabe*
   Mithilfe dieser Funktionalität werden Berechtigungen analog den Unternehmensrichtlinien und gesetzlichen Anforderungen automatisiert, kontrolliert und effizient vergeben. Benutzer können über eine webbasierte Schnittstelle Zugriff auf Anwendungen beantragen. Hierbei wird die Rolle des anfragenden Benutzers mit dem gewünschten Zugriffsrecht abgeglichen und an die zuständige Person zur Genehmigung weitergeleitet. Bereits innerhalb des Genehmigungsprozesses können bestehende Risiken analysiert und beseitigt werden.
3. *Unternehmensweites Rollenmanagement*
   Mithilfe von SAP GRC Access Control erfolgt die standardisierte und zentralisierte Rollendefinition, -anlage und -verwaltung nach vorab definierten Regeln. Rollenkonflikte werden vermieden. Ein unternehmensweites einheitliches Rollenkonzept führt zu einem einheitlichen und anwendungsübergreifenden Rollendesign. Rollen werden automatisch angelegt und dokumentiert. Die Rollen werden von den Geschäftsprozessverantwortlichen definiert und mit den entsprechenden Zugriffsrechten versehen. Dabei können die Prozessverantwortlichen Einblick in alle Rollen haben, die in einer bestimmten Transaktion notwendig sind. Bevor die Rollen aktiv geschaltet werden, prüft SAP GRC Access Control, ob Funktionstrennungsrisiken vorliegen, und macht diese sichtbar.
4. *Management von Superuser-Berechtigungen*
   Diese Funktionalität steuert im Notfall den Zugriff von sogenannten Superusern auf Anwendungen und kontrolliert deren Berechti-

gungen, damit es zu keinen Compliance-Verstößen kommt. Die Superuser-Berechtigungen ermöglichen den privilegierten Zugriff auf Anwendungen mit eingeschränkter Gültigkeit. Alle Aktionen finden in einer kontrollierten und prüffähigen Umgebung statt und werden detailliert protokolliert.

5. *Regelmäßige Überprüfung der Zugangskontrollen*
   SAP GRC Access Control ermöglicht die regelmäßige Überprüfung der Berechtigungen von Benutzern im Hinblick auf Funktionstrennungsrisiken. Hierbei wird sichergestellt, dass alle Berechtigungen regel- und gesetzeskonform vergeben wurden und die Beseitigung von Funktionstrennungskonflikten nachweisbar ist.

Mithilfe der beschriebenen Funktionalitäten werden unberechtigte Zugriffe auf Prozesse und der Missbrauch von Berechtigungen verhindert. Kosten und Zeitaufwand für interne und externe Prüfungen im Hinblick auf die Erfüllung der Compliance-Anforderungen werden signifikant reduziert. Das Rollenmanagement und die Berechtigungsvergabe können kostengünstiger und effizienter geleistet werden. Präventive und detektive Kontrollen ergeben gemeinsam mit der Automatisierung der Compliance-Prozesse ein optimiertes und effizientes internes Kontrollsystem. Das effiziente Management der Compliance wird durch ein kontinuierliches Monitoring und Reporting abgerundet, das dem Management jederzeit den aktuellen Status der Compliance-Aktivitäten liefert.

5 Pro und Kontra der Lösung

Entscheidungen über eine Investition in die IT-Compliance sind gegenwärtig von zwei Extremen geprägt. Entweder werden die Kosten einer konsequenten Umsetzung überschätzt oder die Konsequenzen der Nichteinhaltung gesetzlicher Normen und Vorschriften unterschätzt. Eine daraus resultierende Kosten-Nutzen-Überlegung führt oft zu falschen Entscheidungen. Dabei können sich die Unternehmen durch eine effiziente und effektive Umsetzung der Zugriffskontrollen und nachhaltigen Compliance einen komparativen Wettbewerbsvorteil erarbeiten, indem sie langfristig Kosten reduzieren und einen Reputationsbonus realisieren – wie es am Beispiel der GRC-Tools deutlich wird.

Selbstverständlich sollen dabei die Fixkosten der Investition in die Analyse, Lösungsfindung und Umsetzung nicht unterschätzt werden. So erfordern die GRC-Tools ebenfalls Wartung und Pflege, und Mitarbeiter, wie das technische Personal, müssen im Umgang mit den Lösungen geschult werden.

Diese Compliance-Lösung ist daher eine strategische Investition, die einen signifikanten Mehrwert auf der Business-Unit-Ebene darstellt und sich weniger deutlich auf z.B. Transaktionskosten auf der IT-Ebene auswirkt. Nicht immer spart man bei einer Automatisierung ad hoc so viel, wie man annimmt. Die Wettbewerbsvorteile können hier i.d.R. erst über mehrere Perioden realisiert werden.

6 Literatur

[Barnier 2009] *Barnier, B.:* Driving Value From Non-revenue-generating Activities: Myths and Misunderstandings of Governance and Risk Management. ISACA Journal 2 (2009), S. 37–43.

[Götz et al. 2008] *Götz, B.; Köhntopp, F.; Mayer, B.; Wagner, G.:* Einsatz einer ganzheitlichen GRC-Softwarelösung. HMD – Praxis der Wirtschaftsinformatik 45 (2008), 263, S. 89–107.

[IDW 2002a] *IDW:* Prüfungsstandard – Abschlußprüfung bei Einsatz von Informationstechnologie (IDW PS 330) vom 24.9.2002.

[IDW 2002b] *IDW:* Stellungnahme zur Rechnungslegung – Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1) vom 24.09.2002.

[Kloock & Sabel 1992] *Kloock, J.; Sabel, H.:* Economies and Savings als grundlegende Konzepte und Erfahrung. Was bringt mehr? Zeitschrift für Betriebswirtschaft 63 (1993), S. 209–233.

[Mehta 2009] *Mehta, A.:* Compliance Audit – A Process of Optimization, Not an Obligation. ISACA Journal 1 (2009), S. 37–38.

[Norris 2003] *Norris, P.:* Young People & Political Activism: From the Politics of Loyalties to the Politics of Choice? Conference paper for Council of Europe Symposium, Strasbourg, Nov. 2003.

Dipl.-Betriebswirt Sven Petermann
ESPRiT Consulting AG
Bavariaring 28
80336 München
sven.petermann@esprit-consulting.com
www.esprit-consulting.com

Dr. Aleksandra Sowa
Deutsche Telekom AG
Friedrich-Ebert-Allee 140
53113 Bonn
www.telekom.de