Steffen Weitz

Christoph Wildensee

Revision

Generischer Implementationsansatz von IKS-Kontrollstrukturen in Micro-services-basierten Anwendungen aus Sicht der Internen Revision

1. Einleitung

In vielen Unternehmen sind monolithische IT-Systeme wie SAP im Einsatz. Ein so funktional umfangreiches System bietet im Standard bereits für die betriebswirtschaftlich wesentlichen Informationsverarbeitungsebenen eines Unternehmens bzw. eines Konzerns entsprechende IT-Funktionalitäten, d. h. von der Prozessabbildung mit Workflow-, Freigabe- und Berechtigungskonzeptverfahren über die Werteflussdarstellung bis zur Nachweisführung der Geschäftstätigkeit, Erfolgsermittlung und Besteuerungsbemessung bieten solche Systeme üblicherweise transaktionsbasierte Code-Implementierungen. Besondere Erfordernisse in der IT-Abbildung bestimmter Branchen werden über „Industrial Solutions“ offeriert, die sich nahtlos in die Strukturen der Software einpassen. Und auch standardisierte Schnittstellen zur Datenversorgung von/in Drittprodukte sind in solche Systeme integriert.

„Die Führungsfunktion im Unternehmen erfordert die Konzentration des Managements auf kreative und strategische Tätigkeiten. […] Der umfassende IT-Einsatz und die Einführung neuer Organisationsformen haben zu Änderungen der Organisationsstrukturen und -abläufe geführt, wodurch es für die zentrale Unternehmensführung zunehmend problematischer wird, die Gesamtübersicht zu behalten."[1] Dies führt u.a. dazu, dass sie „die Prüfungsfunktion nicht mehr selbst ausüben kann und im Gegenzug ihr Interesse an den Prüfungsinformationen steigt."[2] So überträgt das Management vornehmlich aus Zeitmangel und fehlendem Spezial- und Methodenwissen Überwachungs- und Prüfungsaufgaben an dezidiert hierfür eingerichtete Bereiche wie z.B. die Interne Revision.[3] Allerdings sind die operativen Fachbereiche in erster Linie für die Definition ihrer Prozesse und auch der risikominimierenden organisatorischen und ggf. auch technischen Maßnahmen (zumindest als Initiator) im Sinne eines einzurichtenden Internen Kontrollsystems (IKS) verantwortlich, sodass sie diese Maßnahmen auch zwecks Ordnungsmäßigkeitsnachvollzug und „Exkulpation" zu dokumentieren haben. Dies betrifft insbesondere ebenso die Allokation der Prozessschritte mit der jeweils zugehörigen IT-Abbildung. Die Aufgabe der Internen Revision ist es also nicht, ein IKS für das Unternehmen aufzubauen, sondern vielmehr, die operativen Fachbereiche in der Erstellung zu beraten und die Umsetzung dort regelmäßig auf Angemessenheit, Vollständigkeit, Wirksamkeit, Wirtschaftlichkeit und Compliance-Konformität zu überprüfen. Das IKS, das als Managementinstrument zur Sicherstellung der Bereiche „Prozesse", „Informationen", „Vermögensschutz" und „Compliance" gesehen werden kann[4], sollte umgesetzt und betrachtet werden als eine bis ins Detail prozessual aufgebaute Übersicht aller im Unternehmen implementierten technischen und organisatorischen Kontrollen mit entsprechenden Verantwortungszuweisungen auf die operativen Fachbereiche.[5] Zur Mangelbeseitigung werden Maßnahmen definiert, die den verantwortlich handelnden Personen im Unternehmen zur termingerechten Umsetzung auferlegt werden.[6] Das IKS „soll alle primären und sekundären Geschäftsaktivitäten durchdringen, indem es jeweils auf die wichtigsten Risiken ausgerichtet wird und damit zur Zielerreichung beiträgt."[7] Es ist als Prozess ohne limitierend-organisatorische Eingliederung zu implementieren, das die gesamte Wertschöpfungskette durchdringt und in die verschiedenen Geschäftsprozesse einzubeziehen ist.[8] Das IKS kann folgend „zum Frühwarnsystem, das Fehlentwicklungen rechtzeitig aufzeigt und vermeiden hilft"[9], ausgebaut werden. Als zu verknüpfender Grundstock zu einem expliziten Risikomanagementsystem aus Sicht des § 91 Abs. 2 AktG ist dies nicht uninteressant. Eine, wenn auch nicht die einzige der Funktionen im Unternehmen, die eine IKS-Dokumentation als Basis nutzen, ist die Interne Revision – eine zweite Instanz der Wirtschaftsprüfer (WP), der im Rahmen seiner Jahresabschlussprüfung und damit einhergehend der darin enthaltenen IT-Vorprüfung auf die Definition eines systemimmanenten IKS und die Einhaltung der IKS-Grundsätze und konkreten Maßnahmenumsetzungen großen Wert legt. Daher lässt er sich neben eigenen investigativen Bemühungen häufig zusätzlich die Revisionsberichte des abgelaufenen Wirtschaftsjahres vorlegen, um einschätzen zu können, in welchen Bereichen eine Prüfung lohnt bzw. welche Bereiche bereits mit welchen Ergebnissen betrachtet wurden.

Weder die Interne Revision noch der WP kämen auf die Idee, die Gesetzeskonformität eines im Standard eingesetzten IT-Systems wie z.B. SAP und die darin enthaltenen IT-Abbildungen anzuzweifeln. Es ist davon auszugehen, dass dort die Bedingungen zum gesetzeskonformen Einsatz eingehalten werden. Dies betrifft die Vorgaben aus HGB und AO, GoBD, IDW- / FAIT-Vorgaben etc. Lediglich dort, wo ein System angepasst wird, laufenden Veränderungen unterworfen ist (z.B. auch in der Zuweisung von rollenbezogenen Zugriffsberechtigungen und bei vom Unternehmen zu etablierenden IKS-Definitionen) und hauseigene rechnungslegungsrelevante Prozessimplementierungen aufweist, muss gezielt geprüft und die Compliance der IT-technischen Ergänzungen festgestellt werden.

Doch welcher Ordnungs- und Handlungsrahmen gilt, wenn ein wesentlicher Hauptprozess aus der IT-Standardimplementierung herausgelöst und in einer technologisch neuen Umgebung orchestriert wird? Wie muss das IKS ausgeprägt und gehärtet werden[10], damit es innerhalb der energiewirtschaftlichen Prozessabbildung die Grundprinzipien eines ordnungsgemäßen Betriebs aus der Sicht der Internen Revision und des WPs erfüllt?

1 Peemöller/Kregel (2010), S. 2.
2 Peemöller/Kregel (2010), S. 2.
3 Vgl. Peemöller/Kregel (2010), S. 3.
4 Vgl. Wirth (2014), S. 3.
5 Vgl. auch Hunziker (2014), S. 31ff., 62ff., 67f.
6 Vgl. ISACA (2016), S. 9.
7 Vgl. Wirth (2014), S. 4.
8 Vgl. Ruud/Jenal (2004), S. 1046. Zum Begriff der Kontrolle und der deutschen Sicht vgl. Wirth (2014), S. 5f.
9 Peemöller/Kregel (2010), S. 4.
10 Die detaillierte IKS-Übersicht ist Bestandteil der Verfahrensdokumentation. Vgl. BMF (2014), S. 22f., 32.

2. Rahmenbedingungen

Das Lizenzmodell von SAP bedeutet für Unternehmen in Deutschland einen nicht unerheblichen Liquiditätsabfluss pro Wirtschaftsjahr. Das integrative Systemzusammenspiel im Business-to-Customer-Prozess (häufig auch Business-to-Consumer genannt; B2C) führt entsprechend dazu, dass bei den aktuell „niedrigen Spielräumen für Rohmargen“[11] die Cost-to-Serve (Kostenanalysen zur Kundenprofitabilität) sehr hoch sind. So streben die Unternehmen einen höheren Automatisierungsgrad mit geringeren kunden-getriggerten Kosten an.[12] „Zur Verbesserung derartiger Kennzahlen hat es sich bewährt, das Thema Vertrieb in verschiedene Bereiche aufzuspalten“.[13] Eine wesentliche Neuerung kann die Einrichtung eines digitalen Vertriebsstranges in Richtung webbasierter Ansprache sein. „Digitale und digitalgestützte hybride Geschäftsmodelle gewinnen stark an Bedeutung. Vollständig digitale Geschäftsmodelle bilden abseits des eCommerce noch nicht die Mehrheit; der Einsatz von Apps und Serviceplattformen ermöglicht es jedoch auch traditionelleren Unternehmen, neue attraktive Kundensegmente zu erschließen“.[14] Die Neuorientierung dieser begrenzten Aufgabe und damit Teilprozessallokation in Richtung IT-gestützter Automatisierungstechnik eröffnet die Möglichkeit, die technologische Basis zu ändern und z. B. u. a. auch Microservices zu nutzen. Dies bedeutet, dass die Kundenansprache über eine App erfolgen kann (Handy, Tablet etc.) und die Vertragsabwicklung bis zur Zahlung und Rechnungslegung weitgehend automatisiert prozessiert wird. Um solche Möglichkeiten nutzen zu können, wird der Prozess in eine Vielzahl von Teilaufgaben unter Wahrung der „modular continuity“ zerlegt, die als jeweiliger Microservice umgesetzt werden können.[15] „Jeder Microservice soll eine eigene fachliche Einheit bilden, die so geschnitten ist, dass für Änderungen oder neue Features nur ein Microservice geändert werden muss.“[16] Jeder dieser Services besteht eigenständig, „Vorteil einer Microservice-Architektur ist [also] die Möglichkeit des unabhängigen Deployments der einzelnen Services“[17], und diese können technologisch beinahe beliebig ausgetauscht werden.[18] Lediglich die Kommunikationsattribute (häufig per REpresentational State Transfer; REST[19]) müssen über das Netz bedient werden können. Die „Microservices sind dafür zuständig, mit den anderen Services zu kommunizieren.“[20] Sie „sind ein effektives Modularisierungskonzept. Nur verteilte Kommunikation ermöglicht es, einen anderen Microservice aufzurufen.“[21] Um derartige Datenverarbeitungen ohne nennenswerten Aufbau eigener Infrastruktur zu managen, werden internationale Anbieter wie z.B. AWS und Zendesk genutzt. Besondere Herausforderungen ergeben sich dabei hinsichtlich des Datenschutz- (Data Processing Agreement, DPA, aus General Data Protection Regulation, GDPR [EU-DSGVO]) und Vertragsrechts (z.B. hinsichtlich der Basisnutzung von Infrastructure as a Service[22], Service-Level-Agreement (SLA)-Festlegung, Gerichtsstand bei Streitigkeiten, Paypal-Integration etc.). Hier endet es jedoch nicht – die Integration von Analytics-Funktionalität (von der Zielgruppen- bis zur Kündiger- und Rückgewinnungsanalyse / Churn Prediction & Prevention und Reduzierung der Churn-Rate) ist nur ein Beispiel für umfangreich datenbasierte Prozessinteraktionen.

Dieses Vorgehen ist eine der wenigen Möglichkeiten, sich im Markt abzugrenzen und eine innovative Produktplatzierung und Kundeninteraktion bei einer geplant geringeren Kostensituation ohne Integration der bisher wesentlichen IT-Kostentreiber zu etablieren. Und es bietet als Ausbaustufe die Möglichkeit, später selbst „Software as a Service“ für Dritte und für verschiedenste Services als jeweils eigene Instanz anzubieten. Die Umgebung ist skalierbar und entsprechend weitgehend unabhängig von der Größe des Verarbeitungsumfangs, der mit dem neuen Technologieeinsatz substituiert wird.[23]

Gehen wir davon aus, dass Microservices entweder über einen Dienstleister, durch eigenes Fachpersonal oder eine Mischung hieraus (insbesondere hervorzuhebender Vorteil des Know-how-Transfers) erstellt und gewartet werden, die in einer solchen Umgebung als Prozesskette je Produkt- bzw. End-to-End-Prozess-Variante als Sequenz definiert und orchestriert werden, bedeutet dies, dass es sich nicht um Standardsoftware handelt, sondern bewusst um eine rechnungslegungsrelevante Eigenentwicklung im Cloud-Umfeld.

11 Lüers/Credo (2010), S. 3.

12 Vgl. auch Warg/Weiß/Engel (2015), S. 19.

13 Lüers/Credo (2010), S. 3.

14 Warg/Weiß/Engel (2015), S. 7.

15 Vgl. Theis (2018), S. 15ff. Vgl. zu Softwarequalitätskriterien auch z. B. Rentschler (2015), S. 55f.

16 Wolff (2016), S. 44.

17 Wolff (2016), S. 75.

18 Vgl. Wolff (2016), S. 61, 78.

19 Vgl. Williams (2015).

20 Wolff (2016), S. 89.

21 Wolff (2016), S. 59.

22 Vgl. hierzu Kirshner/Rappaport (2017), S. 4ff.

23 Vgl. auch Wyman (2018).

3. Aspekte des generischen IKS

Ist der Aufbau des technischen Umfeldes mit erfolgreicher Prozessierung der Daten von der Produktplatzierung und Kundenansprache über den Vertragsschluss, dem Prozessdatenaustausch/-meldewesen (EDIFACT) bis zur Rechnungsstellung und Abrechnung vorhanden, ist es wichtig, die kleinteiligen Prozessschritte mit einem IKS zu belegen. Dieses soll auf jeder Ebene der Anspruchsberechtigten feststellen, ob eine korrekte Abarbeitung stattgefunden hat. Die Controls bedeuten zum einen technische Exception-Feststellungen, die vom IT-System den verantwortlichen Rollenwahrnehmungen gemeldet werden. Ferner bedeutet es auch ein Quittierungsmodell zum Nachvollzug durchgeführter Kontrollen durch die verantwortlich Handelnden. Das nachfolgende Modell zeigt die Grundzüge. Es ist generischer Natur und nicht produktspezifisch oder gar ein ER-Modell. Es kann in beliebige Strukturen eingebettet werden. Kernpunkte sind die Festlegung eines Funktions-Clusters und die Zuweisung von Control-Cluster-Definitionen zu den jeweiligen Funktionen.

3.1 Elemente

Übergeordnete Prozesse entsprechen den horizontalen Verantwortlichkeiten im Unternehmen. Beispiele hierfür sind der Vertrieb (B2C und B2B als Segregation), Finanzen, Controlling, Logistik etc. Darunter gliedern sich die Prozess- und ggf. Produktlinien des Unternehmens, die als eigenständig erkannte, wesentliche Ergebnisebenen zu sehen sind. Im Bereich des Vertriebs entspricht dies den spezifischen Customer Journeys, d.h. jedem einzelnen Erlebnisstrang innerhalb der Produktwelt bzw. auch den End-to-End-Prozessen des Unternehmens zum Kunden. Jede dieser Ebenen wird durch verantwortliche Produkt- oder Prozess-Owner repräsentiert. Sie übernehmen die Verpflichtung, diese Stränge Compliance-konform zu halten und benötigen u.a. ein aussagefähiges Sicht-Cockpit bzw. Dashboard zur Identifizierung bei IKS-Verstößen. Jeder übergeordnete Prozess hat eine 1:n-Referenz auf die nachfolgende Ebene, die wiederum eine 1:n-Referenz auf die funktionale Ebene aufweist. Die Festlegung der Stränge erfolgt auf dieser zweiten Ebene mit den Elementen der dritten Ebene, die die Funktionen des Funktions-Clusters zu sequentiellen Abarbeitungen zusammenfassen. So entstehen also Datenverarbeitungsdefinitionen (Prozess- und Produktstränge), die sich jeweils als Sequenzreihe der einzelnen Funktionen des Funktions-Clusters zusammensetzen (z. B. Prozess 1 wie in Abbildung 1). Dies entspricht der Kommunikation der einzelnen Funktionen untereinander, die als Aufgaben-/Teilprozessdefinitionen mit Microservices-Abgrenzungen gleichzusetzen sind. Im operativen Geschäft erfolgt die Verantwortungsübernahme vertikal über die Funktionsgruppenebene (als Kategorisierung der Verantwortlichkeit) in die Funktionen hinein. Hier muss ein Detailwissen über die Funktionalität der Teilprozessabgrenzungen/Microservices vorhanden sein, um diese über zu definierende Controls zu steuern bzw. fehlerhafte Verarbeitungen als Exceptions identifizieren zu können.

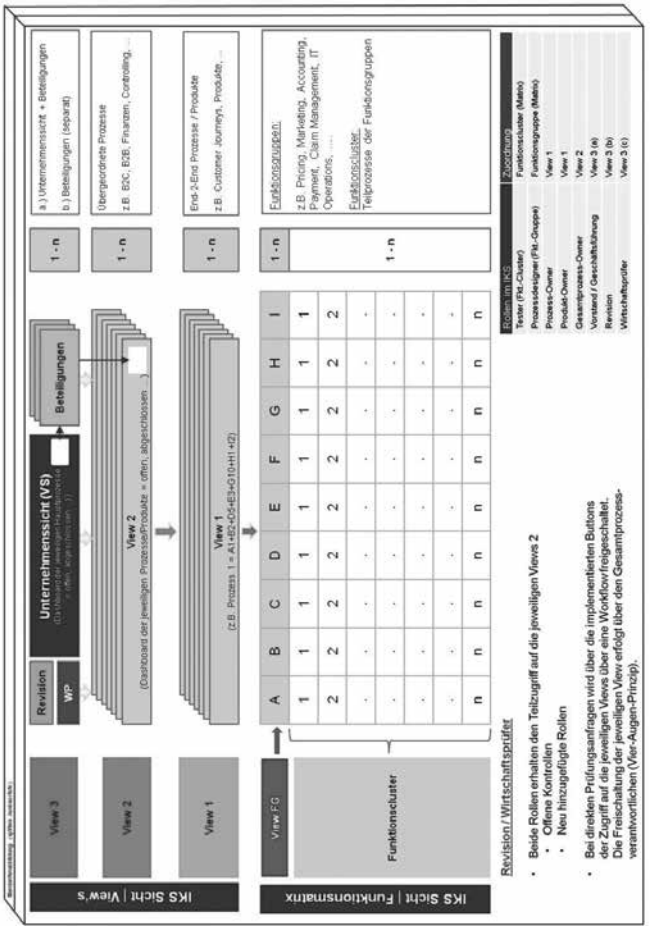

Abb. 1: Generischer IKS-Ansatz.

Die einzelnen Funktionen benötigen eine 1:n-Beziehung zum Control-Cluster. In diesem werden alle zu definierenden Controls (auch Single Control Actions genannt), seien es Datenanalysen/-bereitstellungen oder nur manuelle Schritte, gehalten. Den Funktionen werden sie als Auszug der Gruppe einplanungssensitiv zugewiesen. Jede Funktion – mit Referenz zur übergeordneten Unternehmensrisikomatrix – hat also ihren individuellen Control-Zuweisungsblock und eine Definition der Verarbeitungsreihenfolge der Controls.

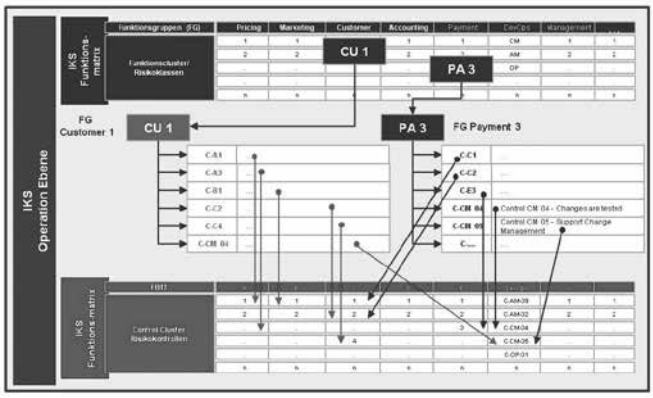

Abb. 2: Detailsicht auf das Control-Cluster.

Eine Funktionsgruppe besteht aus mehreren Funktionen im Funktionscluster (1:n). Die Funktionen selbst referenzieren wiederum auf unterschiedliche Risikokontrollen des Control-Clusters – unabhängig von der Funktionsgruppenzuweisung der Control (1:n). Die Risikokontrollen können also unterschiedlichen Funktionen zugeordnet werden. Dies klingt zunächst wie ein Widerspruch, ist aber aufzulösen. Das Ziel ist, dass eine Control zwar einer Funktionsgruppe thematisch zugehörig ist und somit in der Ausgestaltung dort verantwortet wird, sie aber trotzdem aus verschiedenen Funktionen heraus getriggert werden kann. Innerhalb einer Funktion können also auch Controls einer anderen Funktionsgruppe eingeplant werden. Entsprechend ist bei der Auslösung der Control die auslösende Funktion (und daraus abgeleitet die Funktionsgruppe) mitzugeben. Diese Flexibilität ist eines der wesentlichen Elemente des Designs.

3.2 Views und Dashboards

Verantwortlich handelnde Personen benötigen verschiedene Sichten auf die Kontrollschicht. Während auf der Ebene der Funktionsgruppen, also der operativen Verantwortlichkeit, eine nach Wahl eines Stranges notwendige Detailsicht möglich sein muss, die klar darlegt, in welchem Microservice welche Control eine Exception ausgelöst hat und welche Wirkung dies in welchem Prozess- oder Produktbild bedeutet, benötigen die Ebenen darüber zunächst weniger Detailschärfe, als vielmehr Dashboard-Ansichten. Verantwortliche Personen können sich dann bei den nachfolgend Verantwortlichen informieren.

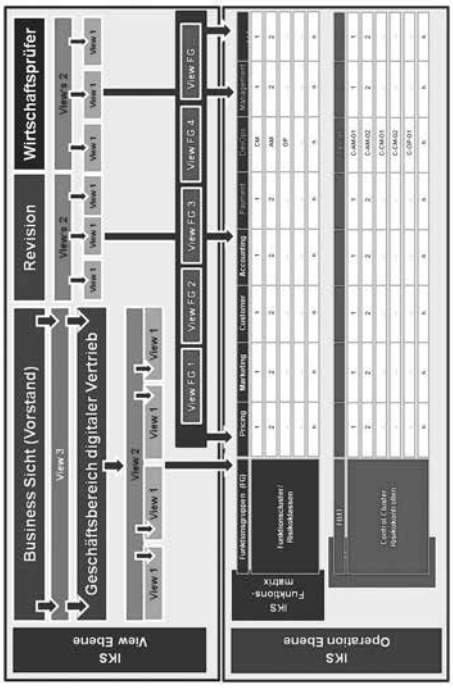

Abb. 3: Verschiedene Sichten in das Control-Cluster.

Gleiches trifft auf die Funktionen Interne Revision und Wirtschaftsprüfer zu. Auch hier wird eher eine Dashboard-Sicht angestrebt, allerdings muss es, ggf. mit einer Freigabestrategie, die eine dezidierte Sichterlaubnis der Verantwortlichen bedeutet, möglich sein, dass eine Detailsicht auf die Fehlerquellen stattfindet. Um eine Gesamtsicht je Gruppierungsebene zu erhalten, müssen mehrere Status abgebildet werden, so mindestens „Exception offen“, „in Bearbeitung“ und „fertig/unkritisch“.

Eine Besonderheit stellt die Unternehmenssicht dar (Vorstand/Geschäftsführung). Mit Blick auf heutige Unternehmen, die in Konzernstrukturen eingebettet sind und dabei sehen müssen, ob in Beteiligungen Exceptions ausgelöst werden, muss ein Dashboard eine Konzernstruktur in Grundzügen bzw. übergeordnet abbilden können. So kann eine Orchestrierung des funktionalen Umfeldes Elemente hervorbringen, die multipel bzw. auch unternehmensübergreifend eingesetzt werden, z. B. zur Rechnungserstellung, Steuerbemessung, Verbuchung etc. Ist dies der Fall, muss ebenfalls die auslösende Konzernebene aus dem Exception-Handling der funktionsgetriggerten Controls hervorgehen.

	View FG	View 1	View 2	View 3
Verantwortung	Operative Verantwortlichkeit auf der Ebene der Funktionsgruppen (Fkt.-Gr.)	Verantwortet Prozess- oder Produktsicht, Zugriff auf Fkt.Gr.	Identifizierung der Prozess- und Produktverantwortlichen ausreichend	Geschäftsführung, Identifizierung aller Verantwortlichen
Sichtebene	Drill-Down von Funktionsgruppe bis auf Control-Ebene, Exception-auslösende Konzernstruktur inklusive	Dashboard auf beteiligte Fkt.-Gr., Prozess- oder Produktebene, „Customer Journey“	Dashboard aller – auch übergeordneter – Prozesse, Abgrenzung zu integrierten Konzernprozessen möglich	Dashboard aller Prozesse, separate Sicht auf vorhandene Beteiligungen
Revision/WP	Durchgriff auf Fkt.-Gr. und Control-Ebene nach Freigabe durch Verantwortliche		Standardsicht ohne Freigabestrategie	Auswahl als ergänzte Sicht nicht nur über Fkt.-Gr., sondern über alle Prozess- und Produktsichten nach Freigabe

Tab. 1: View-Ebenen

Zu sehen ist also, dass die verschiedenen Views und Dashboards als Ableitung der unterschiedlichen Sichten der hierarchisch verantwortlich Handelnden auf die Prozess- oder Produktebene und daraus folgend bis auf die Kontrollebene zugreifen und dabei die Informationstiefe abgestuft bedienen können müssen. Ein Drill-Down muss implementiert werden und den operativ Verantwortlichen wie auch den Organen der Selbstkontrolle zur Verfügung stehen. Entwickler und Tester benötigen weniger die aggregierte Sicht der Produkt- oder Prozess-Owner als vielmehr ausdrücklich die Sicht auf die operative Ebene. Alle Views benötigen also den vollen Zugriff auf die Funktions- und Kontrollcluster, damit auf jeder Ebene die verschiedenen Kritikalitätsübersichten erstellt werden können. Allerdings werden die Cluster im Bereich des Management-Dashboards ausgeblendet, und auch die Revision und der Wirtschaftsprüfer bekommen ggf. nur nach Freigabe durch die Verantwortlichen eine Einblendung mit Detailsicht auf den Control-Cluster.

3.3 Audit-Strategie bei technischen Änderungen

Eine der wesentlichen Fragen bei Eigenentwicklungen (siehe als Rahmengeber und Beurteilungsbasis zur Ordnungsmäßigkeitsfeststellung insbesondere IDW PS 330 [Abschlussprüfung bei Einsatz von Informationstechnologie], 850 [Projektbegleitende Prüfung bei Einsatz von Informationstechnologie], 880 [Die Prüfung von Softwareprodukten], 951 [Die Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen], RS FAIT 1 und 2 [Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie *und* … Electronic Commerce] und aktuell 860 [IT-Prüfung außerhalb der Abschlussprüfung]) ist die, wie mit technischen Änderungen der definierten Services umgegangen wird. Da die Softwarelösung als Ganzes (direkt oder über Schnittstellenbedienungen) rechnungslegungsrelevant ist und die technischen Festlegungen die Basis der zugrundeliegenden, zwingend notwendigen WP-Softwarezertifizierung bilden, muss vor der Freischaltung jede Funktionalität initial und auch bei Änderungen auf Compliance-Konformität geprüft werden. Es ist darauf zu achten, dass im Verfahren der Freigabeprozess so gestaltet wird, dass die operative Ebene nicht unnötig gestört wird. Gleichsam ist sicherzustellen, dass nur freigegebene Programmierungen und Prozessabläufe aktiviert werden können.[24]

Die Dynamik des Deployments bedingt, dass die operativ Verantwortlichen gemeinsam mit den Prozess- und Produkt-Ownern und der Revision laufend intensiv zusammenarbeiten. Der WP wiederum prüft jährlich im Rahmen der Jahresabschluss-IT-Vorprüfung das Änderungsverfahren und die Prozess- und Implementierungsneufassungen und -änderungen.

4. Besonderheiten aus Sicht der Internen Revision

Die Anwendung dieses generischen Vorgehensmodells, das der Verantwortliche für „digital Governance & Privacy“ des Projektes mit der Revision gemeinsam entwickelt hat, ist eine Möglichkeit, als Revision nah an der Neuentwicklung beteiligt zu sein. Die Impulse der Internen Revision in Richtung Rechtskonformität (rechnungslegungsrelevante Prozesse, GoBD, IDW etc.) sind für das Projekt bedeutsam, um frühzeitig Berücksichtigung zu finden und den nachgelagerten Aufwand zu minimieren. Der Datenschutzbeauftragte des Unternehmens, z. B. hinsichtlich der Vertragswerke im internationalen Umfeld, und der Wirtschaftsprüfer als beratende Instanz sollten ebenfalls einbezogen werden. Für die Revision hat es den Vorteil, dass eine Prüfung erleichtert wird, denn Know-how in diesem Bereich aufzubauen ist nicht trivial, zumal das Deployment und auch die Implementierung solcher Verarbeitungslogik

24 Vgl. z.B. Wildensee (2015), S. 24ff.

erheblich zu bisher im Einsatz befindlichen monolithischen Legacy Systemen differieren. So bleiben dabei die Änderungszyklen dauerhaft bestehen, ein Ende des Deployments kann es aus der Sicht eines Lifecycle-Designs der Prozesse und der ständigen Sicht auf die kundenzentrierten Designs und Changes nicht geben.[25] Daher bedeutet das Integrieren einer Kontrollebene, die hierarchisch different Informationsbedarfe bedient und eine workflow-basierte, historisierte Kontroll-Quittierungslogik beinhaltet (per möglicher Integration einer IKS-Automatisierung, z. B. mit JIRA[26]), sowohl für die Revision als auch den WP, dass spätere Kontrollen[27] effizienter durchgeführt werden können und ein ständig auswertbarer Nachvollzug über risikoklassifizierte Kontrollaktivitäten vorhanden ist. Entsprechend geht diese Kontrollebene erheblich über Monitoring-Informationen aus dem Systembetrieb hinaus.[28]

Durch den Charakter einer solchen Projektumsetzung ist es notwendig, dass die Interne Revision jährlich in diesem Bereich kooperativ prüft und alle Anpassungen und Neuerungen des Systemverbundes über die Versionierung einem Audit unterzieht.

Im Laufe der Zeit wird dies im Bereich der Anpassungen, die immer wieder vorkommen werden, sicherlich geringer ausfallen, da bestimmte Services – sofern erst einmal vorhanden – ggf. eher statisch sind. Regelmäßige Erweiterungen des Umfeldes (Prozesse, Produkte, Services) bedeuten aber, dass es für die Revision eine wiederkehrende Aufgabe ist, die in der Jahresaktivitätenplanung berücksichtigt werden sollte.

5. Fazit

Der Wert zukunftsweisender, auch disruptiver Designs setzt sich durch, „IT schwingt sich […] vom Zulieferer von Lösungen und Systemen zur Realisierung der Anforderungen der Fachbereiche, zuvorderst Marketing und Vertrieb, zu einem echten Partner in Designfragen auf."[29] Und „wer seine Kundendaten auswerten kann, der gibt seinen Mitarbeitern die Chance, individueller und damit besser auf die Wünsche der Kunden einzugehen."[30]

Es ist u.a. Aufgabe der Internen Revision, Prozesse des Unternehmens auf Effizienz zu prüfen. Ein solches im Rahmen der digitalen Transformation initiiertes Ausbauprojekt bedeutet, dass insbesondere den risikobehafteten rechnungslegungsrelevanten Prozessen, aber auch dem Thema Datenschutz bei Nutzung internationaler Dienstleister eine besondere Aufmerksamkeit gewidmet wird. Wenn maßgebliche Projekte angestoßen werden, die umfangreiche Strukturänderungen der Daten- und Prozessverarbeitung nach sich ziehen, ist es sinnvoll, dass die Interne Revision mit dem konzeptionierenden Projekt ein Modell zur Integration von IKS-Kontrollstrukturen unter Beachtung sowohl der Technologie- als auch betriebswirtschaftlichen Ebene entwickelt und dies in die Projektergebnisse operativ integriert. Dies kann für zukünftige Projekte als Blaupause dienen. Für den WP wiederum ergibt sich die Ableitung der Compliance-Konformität aus den im Laufe des Prüfjahres als stimmig bestätigten IKS-Dokumentationen (Tickets, Subtasks) und ist insoweit schnell und unkompliziert überprüfbar.

Literatur

BMF (2014): Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD), Gz: IV A 4 – S 0316/13/10003, DOK: 2014/0353090, 14.11.2014, http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf?__blob=publicationFile&v=3 .

Hunziker (2014): Erfolg der Internal Control – Eine empirische Analyse aus Sicht des Managements, Diss. 2014, Universität St. Gallen, https://www1.unisg.ch/www/edis.nsf/SysLkpByIdentifier/4353/$FILE/dis4353.pdf.

ISACA (2016): ISACA-Leitfaden Grundlagen der IT-Revision für den Einstieg in die Praxis, dpunkt-Verlag, https://www.isaca.de/sites/pf736ofd2c1.dev.team-wd.de/files/attachements/isaca_leitfaden_ii_2016_gesamt_screen.pdf.

Kirshner/Rappaport (2017): Cloud Computing, November 2017, PwC Israel, https://www.pwc.com/il/he/events/assets/2017/21-11/Cloud%20computing%20-%20Saas,%20Paas,%20and%20Iaas.pdf.

Lüers/Credo (2010): Vertriebsmanagement im Energiemarkt: Besonderheiten, Herausforderungen und Chancen, White Paper, 16.07.2010, Homburg & Partner, http://www.homburg-partner.com/fileadmin/image_upload/CC_EU__Vertriebsmanagement__neu__06.pdf.

Nygard (2018): Services by Lifecycle, http://www.michaelnygard.com/blog/2018/01/services-by-lifecycle/.

Peemöller/Kregel (2010): Grundlagen der Internen Revision, Standards, Aufbau und Führung, ESV, 2010.

Rentschler (2015): Model Transformation Languages with Modular Information Hiding, Diss. 2015, Karlsruhe (KIT), https://sdqweb.ipd.kit.edu/publications/pdfs/rentschler2015a.pdf.

Ruud/Jenal (2004): Internal Control – Ganzheitliche Interne Steuerung und Kontrolle (ISK), in: Der Schweizer Treuhänder, 12/2004, S. 1045–1050, https://www.alexandria.unisg.ch/61916/1/Internal%20Control.pdf.

Theis (2018): Cloud Native Architecture: FWP Aktuelle Technologien zur Entwicklung verteilter Java-Anwendungen, 2018, Hochschule München.

25 Vgl. Nygard (2018).

26 Vgl. z.B. https://www.ispicio.com/iks-mit-jira (https://de.atlassian.com/software/jira).

27 Vgl. Wirth (2014), S. 319, zur Abgrenzung des Begriffs Kontrolle zum englischen Ausdruck Control.

28 Vgl. Wolff (2016), S. 250f.

29 Warg/Weiß/Engel (2015), S. 7.

30 Wyman (2018).

Warg/Weiß/Engel (2015): Whitepaper: Service Dominierte Architektur (SDA): Die digitale Transformation erfolgreich meistern, Hamburg, November 2015, https://www.researchgate.net/profile/Peter_Weiss13/publication/309903985_Whitepaper_Service_Dominierte_Architektur_SDA_die_digitale_Transformation_erfolgreich_meistern/links/5825e50008aeebc4f8a1de5b/Whitepaper-Service-Dominierte-Architektur-SDA-die-digitale-Transformation-erfolgreich-meistern.pdf.

Wildensee (2015): Änderungen der Rechtsgrundlagen zum Thema Access Management/Zugriffsschutzsysteme in rechnungslegungsrelevanten ERP-Systemen // GoBD, 2015, http://www.wildensee.de/GOBD_Wildensee.pdf.

Williams (2015): Is REST best in a Microservice Architecture?, 18.12.2015, https://capgemini.github.io/architecture/is-rest-best-microservices/.

Wirth (2014): Internes Kontrollsystem (IKS) bei KMU, Diss. 2014, Universität St. Gallen, https://www1.unisg.ch/www/edis.nsf/SysLkpByIdentifier/4252/$FILE/dis4252.pdf.

Wolff (2016): Microservices Grundlagen flexibler Softwarearchitekturen, dpunkt-Verlag, 2016.

Wyman (2018): Nicht nur Start-Ups haben die Chance, den digitalen Wandel zu überleben, Wirtschaftswoche, 22.11.2018, https://www.wiwo.de/adv/oliverwyman/disruption-trifft-tradition-nicht-nur-start-ups-haben-die-chance-den-digitalen-wandel-zu-ueberleben/v_adv/23668408.html.

Dipl.-Ingenieur **Steffen Weitz** war bereits im Projekt enercity digital und nach Überführung in den Bereich Digitalvertrieb bzw. folgend in Sales – Product Management & Marketing für digital Governance & Privacy zuständig. Als Chief Digital Architect ist er maßgeblicher Impulsgeber für wichtige Aspekte des konzipierten Digitalvertriebsstranges. Zuvor arbeitete er sowohl bei der enercity AG als auch in verschiedenen Unternehmen u. a. als IT-Projektleiter.

Dr. h.c. **Christoph Wildensee**, DBA, CISM, CRISC, ist seit vielen Jahren in der Internen Revision der enercity AG, Hannover, tätig. Zwischen 2008 und 2012 war er in Personalunion Datenschutzbeauftragter des Unternehmens und der zugehörigen Netzgesellschaft. Er hält einen Ehrendoktor der polytechnischen Universität aus Pernik (EPU).