Alexander Volland et al. (Hrsg.): Projektmanagement & Vorgehensmodelle 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 81

Reduktion der Dokumentationspflichten für Softwareentwicklung und Softwaredeployment in einem regulierten Umfeld

Timothy Hansen[1] und Alexander Volland[2]

Abstract: Der Artikel beschäftigt sich mit der Reduktion der IT Dokumentationspflichten in einem Unternehmen, welches als Kapitalanlagegesellschaft einer Reihe von verbindlichen externen Richtlinien und selbstauferlegten Vorgaben unterliegt. Über mehrere Jahre sind mit wachsenden Vorschriften redundante Kontrollen und Ergebnistypen mit Überschneidungen etabliert worden, die zwar die Dokumentationspflichten darstellen, in der Praxis jedoch einen hohen Aufwand erzeugen. Vergleichbar mit anderen größeren Unternehmen werden Kontrollen von unterschiedlichsten Funktionen, teils praxisfern, teils praxisnah, definiert und sind dann von Projekten zu erfüllen. In der Ausgangssituation fanden wir neben verschiedenen Tools, in denen Kontrollen abgebildet wurden auch eine sog. Service Acceptance Criteria Liste (SAC-Liste) vor, welche verbindlich 160 Kontrollen für Produktivnahmen enthielt. Mit unserem Vortrag zeigen wir auf, wie die Kontrollen mit einer einheitlichen Struktur und einer übergreifenden Methodik aufeinander abgestimmt und damit Redundanzen sowie Blindleistung erheblich reduziert werden können. Die angewendete Struktur setzt dabei auf folgende Eigenschaften einer Kontrolle auf: Scope, zur Steuerung des Geltungsbereichs; Szenarien bezüglich des Umfangs und Art der Änderung; Quality Gates, die eine Abhängigkeit und eine Abfolge aufzeigen; Fokus auf Ergebnistypen mit Gütekriterien als Kontrolle, klare Benennung der relevanten Verantwortungen hinsichtlich Definition von Kontrollen, Bearbeitung sowie Empfänger und Abnehmer. Diese Kombination ergibt ein leicht darstellbares, pflegbares Kontrollenmodell, welches zugleich eine Reduktion der Kontrollen auf das Wesentliche ermöglicht. Ergänzend wurde ein einfacher, an Lean-Management-Methoden angelehnter Prozess etabliert, mit dem der Neuaufbau von redundanten Prüfungen verhindert werden soll. Zusätzlich sollen die Kontrollen so aufbereitet werden, dass diese zielgerichtet, risikoorientiert und passend für das jeweilige IT-Projekt ausgewählt werden und jeweils zeitnah geprüft werden. Mit Hilfe des neuen Modells kann anhand eines Beispielprojekts nachgewiesen werden, dass die Pflichtkontrollen auf 9 % des ursprünglich undifferenzierten Gesamtumfangs reduziert werden können. Der Artikel stellt das Projekt und das erarbeitete Optimierungsmodell vor.

Keywords: Administrationsaufwand, Dokumentationspflicht, reguliertes Umfeld, Kontrollen

1 Einleitung

Das Unternehmen hat im Rahmen der Softwareentwicklung und des Softwaredeployments umfangreiche Dokumentationspflichten, welche aus internen und externen Vorgaben resultieren.

Um die Vollständigkeit der Dokumentation und damit die Erfüllung der internen und externen Vorgaben zu gewährleisten, wird die Vollständigkeitskontrolle über sogenannte

[1]Union IT-Services GmbH, Release Management, Weißfrauenstraße 7, 60311 Frankfurt/Main, timothy.hansen@union-investment.de
[2]Union IT-Services GmbH, Projekt Management, Weißfrauenstraße 7, 60311 Frankfurt/Main, alexander.volland@union-investment.de

Service Acceptance Criteria (SAC-Liste), mit derzeit 160 Kontrollen durchgeführt. Diese Kontrollen sind für jedes Releasedeployment auf Produktion zu dokumentieren. Dies bedeute im Umkehrschluss, dass für ein komplexes IT-Projekt mit mehreren Produktionsdeployments, etwa über mehrere Systeme hinweg, oder bei agilem Vorgehen mehrere Deployments pro Applikation, diese Liste n-mal bearbeitet werden muss.

Die 160 Kontrollen sind einer Vielzahl unterschiedlicher IT Prozesse entnommen, im Rahmen des Projekts wurden 24 relevante Prozesse identifiziert.

Die inhaltliche Verantwortung für die Abnahmepunkte in dieser Liste liegt beim Prozess *Release Management*; jedoch betreffen nur ca. 10 der 160 Fragen das *Release Management*. Die Prozess-Herkunft der anderen Punkte ist in den meisten Fällen ableitbar, jedoch nicht dokumentiert. Die Pflege der Liste erfolgt regelmäßig jährlich durch Führungskräfte der Betriebsgruppen und einige Prozessverantwortliche von wahrscheinlich beteiligten Prozessen.

Zusätzlich gibt es weitere – teils redundante - Kontrollen, welche in anderen Tools (bspw. dem Projektportfoliomanagementtool) implementiert wurden.

Die Akzeptanz dieser Prüfliste bei den Anwendern im Unternehmen ist eingeschränkt, der Nutzen wird – im Verhältnis zum Aufwand – in Frage gestellt. Eine Analyse hat ergeben, dass regelmäßig 2/3 der Punkte als „nicht relevant“ gekennzeichnet werden. Dies ist ein Indiz dafür, dass die Fragestellungen dieser SAC-Liste nicht aktuell oder generell für die Mehrzahl der IT-Projekte nicht zielführend sind.

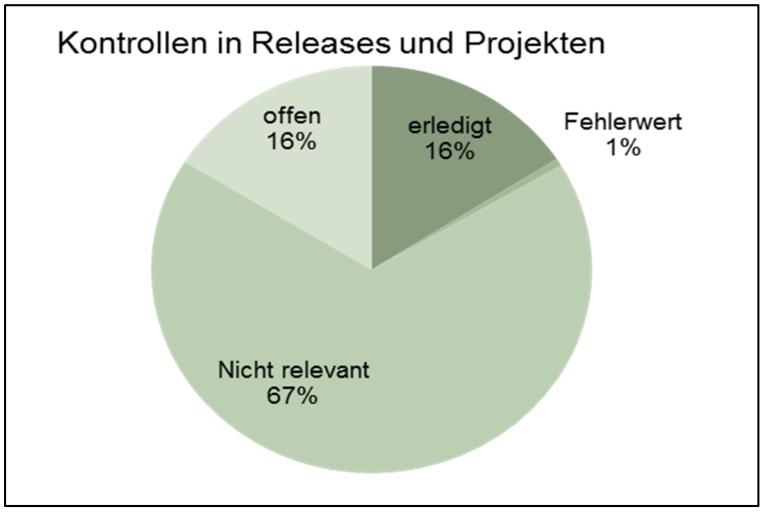

Abbildung 1 - Auswertung der Statuswerte der Kontrollen (Zeitraum 2012 – Juli 2016)

Mit dem in diesem Beitrag vorgestellten Projekt wurden die Kontrollen so überarbeitet, dass nur noch relevante Kontrollen greifen, keine redundanten Abfragen mehr gemacht werden und Kontrollen zeitnah greifen.

2 Ausgangslage und Umfeld

2.1 Trägerorganisation

Das Projekt wurde in einer der größten Fondsgesellschaften Deutschlands durchgeführt. Mit knapp 3000 Mitarbeitern werden über 300 Mrd. Euro Kundengelder in über 4 Millionen Kundendepots verwaltet. Hierfür verwaltet die Fondsgesellschaft über 1.200 unterschiedliche Fonds. Neben ihren deutschen Standorten in Frankfurt am Main und Hamburg ist das Unternehmen außerdem in Hong Kong, Österreich, Luxemburg und Polen vertreten. Für die Projektorganisation ist die interne Strukturierung der IT-Abteilungen relevant:

Die IT-Systeme werden gebündelt in

- Basissysteme (beispielsweise Computer, Telefon, Rechnungswesen, etc.),
- Marktsysteme (beispielsweise Customer Relationship Management, bankfachliche Frontendsysteme, etc.),
- Depotsysteme (beispielsweise Führung der Kundendepots),
- Investmentsysteme (Kauf/Verkauf von Wertpapierpositionen in den Fonds der Fondsgesellschaft).

Jedes Bündel besteht aus 1-3 IT Abteilungen, deren abteilungsübergreifende Zusammenarbeit hauptsächlich innerhalb des jeweiligen Bündels orientiert ist. Die Bündel sind relativ autark voneinander. Daher arbeiten die Abteilungen zwar mit gemeinsamen Prozessen, diese sind jedoch bündelspezifisch ausgestaltet.

Das Unternehmen hat den Anwendungsbetrieb bündelspezifisch in unterschiedliche Rechenzentren ausgelagert. Die Applikationsentwicklung wird in unterschiedlichen Auslagerungsgraden intern gesteuert und extern entwickelt. Genau diese Heterogenität zwischen den Bündeln ist eine weitere Herausforderung bei der Festlegung von IT-Prozessen und damit auch den damit verbundenen Kontrollen und Dokumentationspflichten.

2.2 Interne und externe Vorgaben auf Projekte

Da es sich beim Unternehmen um einen Finanzdienstleiter handelt, unterliegt es den externen Vorgaben der „Mindestanforderungen Risikomanagement“ [Ba12] sowie den „Bankenaufsichtliche Anforderungen an die IT“ [Rö17] ebenfalls von der BaFin herausgegeben. Neben diesen Vorgaben gelten diverse weitere, wie die Grundlagen der ordnungsgemäßen Buchführung [Bu14] (GoBD), die durch das Institut der Wirtschaftsprüfer (IDW) im Rahmen der Stellungnahmen für Rechnungslegung FAIT (IDW RS FAIT 1 bis 5) ergänzt werden. In Summe gibt es damit bei der Veränderung von IT-Systemen umfangreiche Dokumentationspflichten zu beachten.

Die Aufsicht empfiehlt dabei zur Einhaltung dieser umfangreichen Vorgaben sich an gängigen Standards zu orientieren. Zu diesen Standard zählen die IT Infrastructure Library (ITIL), der BSI Grundschutzkatalog [Is17], oder die internationale Norm für Information Security Management ISO 27.001. Das Unternehmen ist daher zusätzlich nach der ISO

20.000 zertifiziert, welche eine aus der ITIL abgeleitete Norm darstellt und hat für den IT Betrieb ein enges Regelwerk entsprechend Norm-Vorgabe etabliert.

Die internen und externen Vorgaben zur Erstellung und Betrieb von Software werden in einer Vielzahl interner Richtlinien operationalisiert, von denen ca. 24 IT-Richtlinien Abnahmekriterien formulieren und daher mehr oder minder für dieses Vorhaben relevant sind:

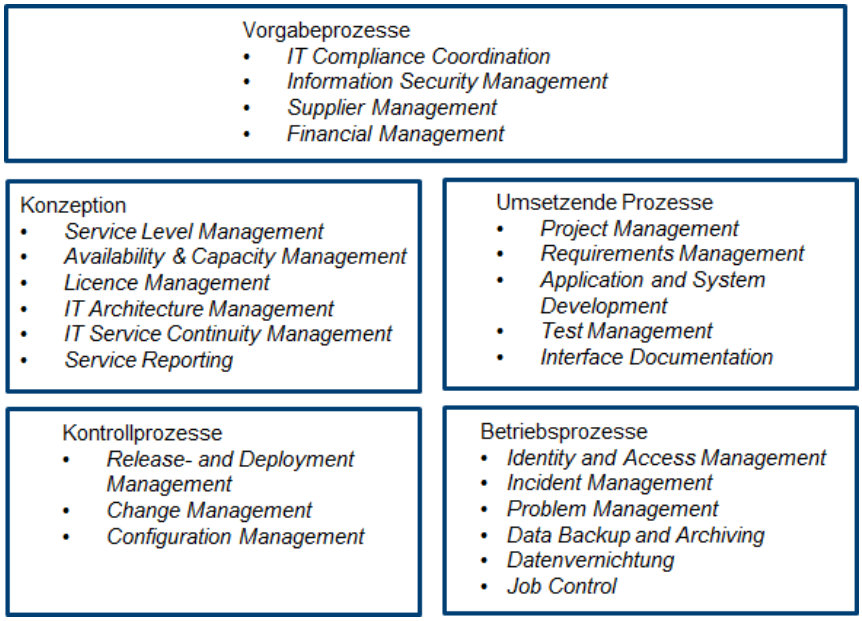

Abbildung 2 - Liste der betroffenen Prozesse

Diese Prozesse wurden von unterschiedlichen Stakeholdern im Unternehmen definiert. Grundsätzlich sind alle Prozesse von IT Projekten verbindlich einzuhalten.

Die Prozesse gelten für alle Projekttypen (agile, nicht-agile, hybride Projekte), sowie für nicht-projekthaft umgesetzte Softwareänderungen.

Für die Prozesse wurde in der Regel ein Process Owner, sowie vier Process Manager (je ein Vertreter pro IT Bündel) festgelegt.

2.3 Problembeschreibung

Prüfpunkte der Prozesse (beispielsweise Anforderungen an ein Fachkonzept) werden als sogenannte Kontrollen bezeichnet.

Die in den Prozessen definierten Kontrollen sind teilweise redundant – beispielsweise stellen *IT Architecture Management, Interface Documentation* und *Information Security Management* Anforderungen an Schnittstellendokumentation –, woraus teilweise widersprüchliche Anforderungen entstanden sind.

Hauptinstrument für Kontrollen ist die SAC-Liste, welche als Excel-Datei verbindlich für jedes Release von IT-Projekten zu befüllen ist. Projekte sind in der Organisation Vorhaben mit einem Volumen von mehr als 200T€. In der SAC-Liste werden derzeit pro Release eines Projekts 160 Kontrollen (bzw. zum Teil nur Checkpunkte) abgebildet. Ein ähnlicher Fragekatalog muss im Rahmen des *Change Managements* zusätzlich beantwortet werden, unabhängig von der Natur des Vorhabens. Diese Fragen wurden im Release und Change Management Ticketsystem abgebildet.

Zusätzlich wurden neben der SAC-Liste unterschiedlichste Systeme etabliert über welche Kontrollen abgebildet werden, woraus neue Herausforderungen (Benutzbarkeit, Redundanz, Aktualität) entstehen.

Weitere Kontrollen wurden im Projektportfoliomanagementtool (Planview) abgebildet und einmalig für alle Systemänderungen eines Projekts beantwortet. Dieses Projektportfoliomanagementtool wird aber nur von Projekten verbindlich verwendet. Kleinen Softwarevorhaben unter der Relevanzgrenze verwenden das System nicht.

Das *Anforderungsmanagement* wird – je nach Bündel (siehe 2.1 Trägerorganisation) – in unterschiedlichen System abgebildet (beispielsweise eine Lotus Notes Datenbank, eine JIRA-Implementierung, SharePoint-Liste, usw.), so dass auch hier Kontrollen bündelspezifisch interpretiert und abgebildet wurden.

Weitere Kontrollen sind in unterschiedlichen Testmanagement-Systemen abgebildet (bspw. JIRA, Microsoft Team Foundation Server (TFS), …)

Durch diese heterogene Abbildung der Prozesse ist die SAC-Liste als übergreifende Auflistung der gültigen Kontrollen nicht immer zutreffend.

Die Aktualisierung/Pflege der Kontrollen in den unterschiedlichen Systemen wird voneinander unabhängig und nicht immer synchron mit der Pflege der Richtlinien durchgeführt. In einzelnen Systemen bilden die Systemverantwortlichen die Prozesskontrollen ohne kontinuierliche Rücksprache mit den Process Ownern ab, woraus sich im Zeitverlauf Qualitätsthemen ergeben.

2.4 Zielbeschreibung

Die Kontrollen sollen als Gütekriterien für Ergebnistypen definiert werden. Auf diese Weise soll die Vielzahl der Einzelfragen klar einem Ergebnistyp zugeordnet werden.

Es soll eine zentrale Datenbank aller relevanten Kontrollen mit klaren Verantwortlichkeiten (Pflegeverantwortung für die Kontrollvorgabe) geben.

Die einzelnen Kontrollen in dieser Datenbank unterliegen damit der Eigentümerschaft und Pflegeverantwortung der einzelnen Prozesse (in der Person der Process Owner).

Redundanzen zwischen den Prozessen werden entfernt. Sollte eine Kontrolle in einer weiteren Richtlinie auch „benötigt“ werden, so wird nur noch auf die neue hauptverantwortliche Richtlinie verwiesen.

Die Kontrollen sollen nicht mehr für alle Softwarevorhaben, sondern nur noch für relevante Softwarevorhaben verbindlich sein. Dabei wird risikoorientiert kontrolliert: Hohes Risiko – viel Kontrolle; geringes Risiko – weniger Kontrolle.

Die Kontrollen sollen zeitnah erfolgen und nicht erst „kurz vor Produktivnahme“, so dass im Fehlerfall nicht mehr nur eine sehr kurze Reaktionszeit auf ein Problem möglich ist. Hierfür wird für die Kontrollen ein Quality Gate Modell eingeführt.

Das neue Kontrollsystem soll pilotiert werden.

Eine Tool-Unterstützung (jenseits von Excel) soll nach erfolgreicher Pilotierung adressiert werden.

In Summe soll der Dokumentationsaufwand sinken und gleichzeitig durch die Aktualität der Vorgaben bessere Projektergebnisse ermöglichen.

3 Aufbau des Lösungsbilds

Die vorhergehende Analyse hat mehrere Optimierungspotentiale des Kontrollenmodells aufgezeigt. Einzelne Punkte wurden im Ist-Prozess zunächst in der Praxis näher beleuchtet, um die tatsächlichen Defizite zu erkennen.

In Summe hat sich ein Lösungsbild gezeigt, welches aus sich aus 5 Maßnahmen zusammensetzt, die im Folgenden näher beschrieben werden.

3.1 Klare Kontrollverantwortung etablieren

Eine wesentliche Schwäche der bisherigen SAC-Liste liegt in ihrer positiv zu erwähnenden Entstehung begründet. Sorgsam arbeitende IT-Mitarbeiter haben die aus den Richtlinien erforderlichen Ergebnisse und Kontrollen im Rahmen von Checklisten gesammelt, über Jahre verfeinert und untereinander weitergereicht. Anschließend sind diese Checklisten aufgrund einer geänderten Vorgabe der ISO 20.000 Norm (Überarbeitung im Jahr 2011) in ihrer bestehenden Form ohne Abgleich gegen die Richtlinien in ein Kontrollframework aufgenommen worden. Dies führte dazu, dass in den Checklisten der eigentliche Bezug zu den Vorgaben der Richtlinien nicht festgehalten wurde.

Im ersten Schritt ist daher essentiell zu klären, mit welcher verantwortlichen Person ein Ergebnistyp, eine Kontrolle inhaltlich in Verbindung steht und dieser Person in die Verantwortung zu heben. Aufgrund der bestehenden Prozessorganisation, die im Wesentlichen die Verantwortung für Dokumentationsanforderungen und Abläufe regelt, wurde die Entscheidung gefällt, ausschließlich die Prozesse (in Person der Process Owner) für die Verantwortung heranzuziehen. Kann kein geeigneter Prozess gefunden werden, so wird alternativ nach Richtlinien und ihren Richtlinienverantwortlichen gesucht, die das betreffende Thema regeln. Greift auch diese Variante nicht, wird die bisherige Kontrolle in Frage gestellt und gestrichen.

Hier hat sich in der Voranalyse gezeigt, dass es Ergebnistypen gibt, die samt Kontrollen klar einem einzelnen Prozess zugeordnet werden können. Auf der anderen Seite stellen

Prozesse Ergebnistypen zur Verfügung, die ausschließlich mit Kontrollen aus anderen Prozessen belegt werden. Am häufigsten treten natürlich die Mischformen dieser beiden Extrema auf. Hieraus haben sich zwei zu definierende Verantwortungen abgeleitet: Die Verantwortung für einen Ergebnistyp und die Verantwortung für eine dafür formulierte Kontrolle.

Zur Klärung der Verantwortung ist es nach einer ersten Vorbereitung notwendig, die einzelnen Punkte der vorhandenen Liste mit den Prozesseigentümern und idealerweise mit den bündelspezifischen Prozessmanagern durchzugehen (vergleiche Kapitel 4) und zu verifizieren. Ergänzend dazu können anhand dieser Zuordnung die Richtlinien und Prozesshandbücher geprüft werden, um die Aktualität der Kontrollen sicherzustellen und weitere mögliche Vorgaben zu identifizieren.

3.2 Quality Gate-Kontrollen ganzheitlich managen

Die Analyse zeigt, dass eine späte Kontrolle der notwendigen Dokumentation kurz vor Rollout eines Releases zwar aufzeigen kann, was fehlt, aber nicht rechtzeitig fehlende Punkte heilen kann. Auch die frühe Kenntnis der Soll-Punkte in einem Projekt hat nicht den gewünschten Nutzen erzielt.

Daher ist es naheliegend, einzelne Kontrollen unter Nutzung der im Unternehmen definierten Quality Gates über die Projektlaufzeit zu verteilen. Die Quality Gates lauten in diesem Fall:

- Quality Gate 1: Vorhabenreife
- Quality Gate 2: Umsetzungsreife
- Quality Gate 3: Testreife
- Quality Gate 4: Produktionsreife

Ein weiterer essentieller Baustein ist nun, die auf den anderen Quality Gates liegenden zusätzlichen Kontrollen in die Betrachtung einzubeziehen und eine gemeinsame, ganzheitliche Lösung anzustreben. Hier wurden im Rahmen der Quality Gates 1 und 2 diverse „Checks“ identifiziert, die mit den Verantwortlichen näher betrachtet wurden:

- ITSM-Check (Anforderungen an das Service Management)
- Security-Check (Sicherheitstechnische Anforderungen)
- Infrastruktur-Check (Anforderungen an die Basisinfrastruktur)
- Outsouring-Check (Anforderungen an Outsourcing)

Diese Checks wurden von unterschiedlichen Organisationseinheiten zu unterschiedlichen Zeitpunkten definiert und in die Organisation gegeben. Meist waren konkrete Probleme bei einzelnen Projekten der Auslöser für einen neuen Check, der von nun an von allen Projekten zu beantworten/prüfen war.

Die relevanten Punkte dieser vier Checks fließen nun auch in die neue, zentrale SAC-Liste ein.

Neben der Notwendigkeit, zu kontrollieren, das heißt im Vorhaben erstellte Ergebnistypen nach dem 4-Augen-Prinzip abzunehmen, hat sich in der bisherigen SAC-Liste gezeigt, dass einzelne Punkte keinen Abnahmecharakter haben. Die zukünftige Lösung soll daher aus zwei Teilen bestehen: Abnahmerelevanten Kontrollen und Checklisten ohne Abnahmecharakter.

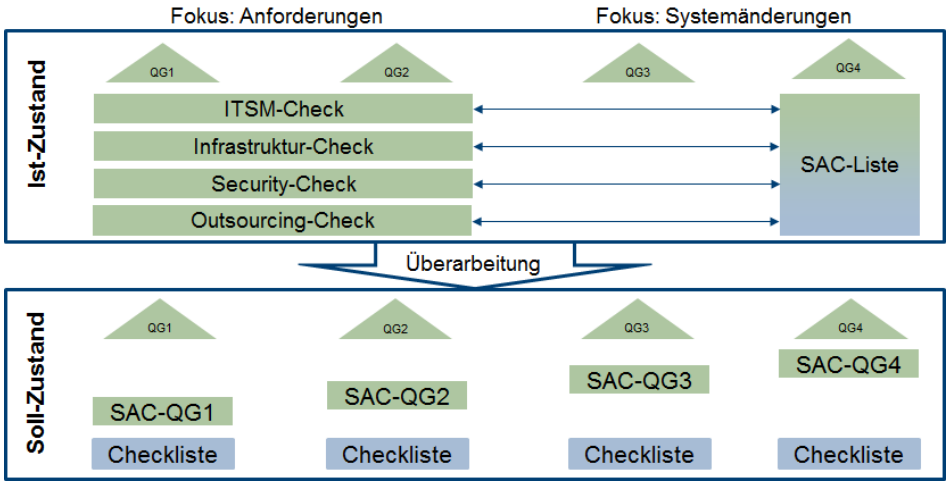

Abbildung 3 - Aufteilung der SAC-Liste in Abnahmeliste und Checkliste über alle Quality Gates

3.3 Auf Ergebnistypen fokussieren

Die bisherigen Kontrollpunkte standen nur bedingt in Verbindung mit den dazugehörigen Ergebnistypen, so dass mehrere Einzelkontrollen mit demselben Ergebnistyp belegt sind. Als Lösung wurde der Fokus auf die Ergebnistypen gelegt, um die Kontrollen zukünftig als Anforderungen an diese Ergebnistypen zu behandeln.

Da jedoch mehrere verschiedene Prozesse Anforderungen an einen Ergebnistypen haben können (geteilter Ergebnistyp), müssen die Kontrollpunkte weiter einzeln in einer Kontrolldatenbank geführt werden. In Zukunft aber sollen Sie jeweils gebündelt mit einem Ergebnistyp abgenommen werden. Aufgrund der Historie der Prozesse, zeigte sich hier schnell, dass es mehrere geteilte Ergebnistypen gibt, die durch die jeweils beteiligten Prozesse recht unterschiedlich gehandhabt werden. So verlangt ein Prozess eine Abnahme seiner Kontrollpunkte, ein anderer Prozess dagegen nicht. Über das methodische Vorgehen (vergleiche Kapitel 4 Methode), konnten solche Widersprüche aufgezeigt und aufgelöst werden.

Mit dem Fokus auf Ergebnistypen wird zusätzlich ein Paradigmenwechsel angestrebt. Auf Basis der Benennung der Ergebnistypen und der erforderlichen Inhalte entfällt zukünftig die Vorgabe von Dokumententemplates, und damit auch, Ergebnistypen als Dokument zu beschreiben. Vielmehr ist es nun möglich, mit Hilfe IT-gestützter Systeme einzelne Ergebnistypen abzubilden und zu dokumentieren. Die Anforderungen an die Nachvollziehbarkeit und die Revisionssicherheit bleiben selbstverständlich unverändert bestehen und müssen damit auch in dieser Lösung berücksichtigt werden.

3.4 Änderungsszenarien einführen

3.4.1 Risikoorientierte Szenarien

Die bisherige Struktur der Kontrollen der SAC-Liste nimmt in ihrer Natur keine Rücksicht auf die Inhalte eines Projekts. Alles kann relevant sein, es kann jedoch auch nur der Pflichtteil relevant sein. Daher lag es im Ermessen der Beteiligten, ob einzelne Punkte als relevant eingestuft werden.

Die Datenanalyse und die Einzelgespräche im Rahmen konkreter Anwendungsfälle haben jedoch gezeigt, dass viele Vorhaben oft recht kleine Anforderungen an die IT-Systeme stellen. Die Ursache ist in der jeweiligen IT-Architektur der Bündel zu finden, die zu folgenden Rahmenbedingungen führt:

1. Aufgrund der fortgeschrittenen IT-Unterstützung der Fachprozesse werden selten neue Systeme etabliert.

2. Die stark vernetzte IT-Architektur führt dazu, dass Projekte Funktionen nur durch Änderung mehrerer IT-Systeme vollständig umsetzen können.

3. Die Releasestrategie sieht eine größtmögliche Entkoppelung der Releases vor, welches über die Schnittstellenarchitektur auf Basis eines EAI-Systems bestmöglich unterstützt wird [SJL08]. Dies führt zu häufigen, kleinen Releases in der Applikationslandschaft.

In der Konsequenz hat sich gezeigt, dass viele Änderungen – auch aus Projekten – je System betrachtet, kleinerer Natur sind.

Hieraus leiten sich vier Änderungsszenarien ab, für die fortan getrennte Kontrollsets definiert werden sollen:

- **Neue Applikation:** Das Szenario ist für den Aufbau neuer Applikationen relevant. Hierfür gibt es umfangreiche regulatorische und hausinterne Dokumentationsvorgaben. Insbesondere der initiale Aufbau der späteren Betriebsdokumentation ist umfangreich.
- **Abschaltung:** Der andere Extremfall ist die Abschaltung einer Applikation. Für diesen Fall gelten besondere Anforderungen, die in den anderen Änderungsszenarien nicht zum Tragen kommen.
- **Änderung:** Die Änderung, beziehungsweise „Normale Änderung“, steht für die alltägliche Weiterentwicklung der Systemlandschaft. Der erforderliche Dokumentations- und Kontrollaufwand ist geringer, als für eine neue Applikation. Jedoch ist es erforderlich, die gesamte Dokumentation für die Applikation nach Bedarf zu prüfen und anzupassen.
- **Kleinständerung:** In Abgrenzung zur Normalen Änderung soll die Kleinständerung besonders leichtgewichtig sein und wenige Vorgaben machen. Um einen solchen Änderungstyp zu etablieren, ist eine schlanke Impactanalyse erforderlich, die klar aufzeigt, wann dieser Änderungstyp greift.

Die Aufteilung nach Szenarien ist dabei ein erster Schritt, ein risikoorientiertes Vorgehen zu etablieren, denn abhängig vom Anwendungsfall soll der Dokumentationsaufwand zugeschnitten werden. Die definierten Ergebnistypen haben durch die hinterlegten Kontrollpunkte eine Besonderheit: Die Szenarien können auf die Kontrollen runtergebrochen werden. So kann ein Ergebnistyp im Szenario Neue Applikation umfangreichere Kontrollanforderungen haben, als im Szenario Änderung.

3.4.2 Zugeschnittene Szenarien

Auch die IT-weiten, risikoorientierten Szenarien führen weiter dazu, dass Ergebnistypen und Kontrollen eingefordert werden, die in bestimmten Situationen nicht passend sind. Da diese unnötigen, undifferenzierten Kontrollen ein besonderes Risiko für die spätere Akzeptanz darstellen, ist auch hier eine Lösung erforderlich. Umgekehrt ist genauso denkbar, dass in anderen Situationen zusätzliche Ergebnistypen und gegebenenfalls auch Kontrollen gewünscht sind.

Daher ist der nächste Schritt die Einführung der genannten Szenarien in Kombination mit weiteren Dimensionen:

- Architektur-Domänen
- Schutzniveaus des Information Security Managements
- Spezifische Applikationslösungen
- Organisationseinheiten
- Kundendomänen
- Ggf. weitere Kriterien

Im ersten Schritt werden für diese Dimensionen verschiedene Ausprägungen konzipiert. So ist es zunächst erforderlich, in den Szenarien Muss- und Kann-Kriterien zu identifizieren. Die Kann-Kriterien gelten nur unter bestimmten Rahmenbedingungen, die ebenfalls zu definieren sind.

Hierbei handelt es sich um einen weiteren großen Verbesserungsschritt. Auf Basis der Kann-Kriterien und der dazugehörigen Bedingungen können anschließend für die genannten Dimensionen Szenarien individuell nach dem übergreifenden Schema zugeschnitten werden.

Dieser Ansatz soll im Rahmen der angestrebten Toolumsetzung vorangetrieben werden. Diese muss dabei einerseits das komplexe Datenmodell dieser verschiedenen Dimensionen abbilden können, und andererseits mit den Muss- und Kann-Kriterien umgehen können. Hierbei ist die damit einhergehende Komplexität zu beachten und zu steuern.

3.5 Redundanzen abbauen

Die Struktur der bisherigen Lösung hatte zur Folge, dass diverse Kontrollpunkte mehrfach redundant abgefragt wurden. Dies hat wesentlich zur mangelnden Akzeptanz beigetragen. Die eigentliche Natur der Redundanzen war jedoch sehr unterschiedlich. Im Wesentlichen konnten zwei Redundanztreiber identifiziert werden:

1. „Echte Redundanz“: Dieselbe Information muss in mehreren Ergebnistypen zu unterschiedlichen Zeitpunkten hinterlegt werden.

2. „Kontrollredundanz“: Eine Kontrolle wird im Rahmen eines Vorhabens mehrmals zu bestimmten Zeitpunkten abgefragt, obwohl für den Inhalt eine einmalige Abfrage ausreichend wäre.

3.5.1 Echte Redundanzen abbauen

Im Rahmen der Überarbeitung hat sich herausgestellt, dass sich die echten Redundanzen zunächst nur bedingt auflösen lassen, da spezifische Rahmenbedingungen das mehrfache Hinterlegen einer Information an unterschiedlichen Stellen erforderlich macht. Als Ursachen wurden identifiziert:

- Einzelne Ergebnistypen sind unterschiedlichen Zielgruppen zugänglich, bestimmte Informationen sollen Zielgruppe A mitgeteilt werden, andere explizit nur Zielgruppe B.
- Fehlende Automatismen für die redundante Dokumentation der Informationen.

Mit der angestrebten Lösung wird zunächst als Ziel verfolgt, diese Redundanzen transparent zu machen, um mittelfristig eine Reduktion zu bewirken.

3.5.2 Kontrollredundanzen abbauen

Als Lösung für die Kontrollredundanz wird für die Ergebnistypen und Kontrollpunkte nun ein Scope definiert, für den sie zur Anwendung kommen sollen. Der Scope definiert, wann und wie häufig eine Kontrolle in einem Vorhaben greift und in welchem Rahmen ein Ergebnistyp tatsächlich zu prüfen und zu aktualisieren ist.

Die Struktur der Organisation, der Prozesse und der Quality Gates hat eine einfache Scope-Klassifizierung ergeben:

- **Vorhaben:** Darunter werden sowohl Projekte als auch weitere geplante Systemänderungen geführt. Ein Ergebnistyp, beziehungsweise Kontrollpunkt auf Vorhabenebene muss in der Regel für das gesamte Vorhaben lediglich einmalig bearbeitet und kontrolliert werden.
- **Applikation:** Die Ergebnistypen und Kontrollen sind applikationsspezifisch. Betrachtet ein Vorhaben mehrere Applikationen, so sind die Kontrollpunkte je Applikation einmal zu durchlaufen.
- **Release:** Die Ergebnistypen und Kontrollen müssen je Release durchlaufen werden, dies beinhaltet insbesondere einen Abnahmetest und einen Rollout.

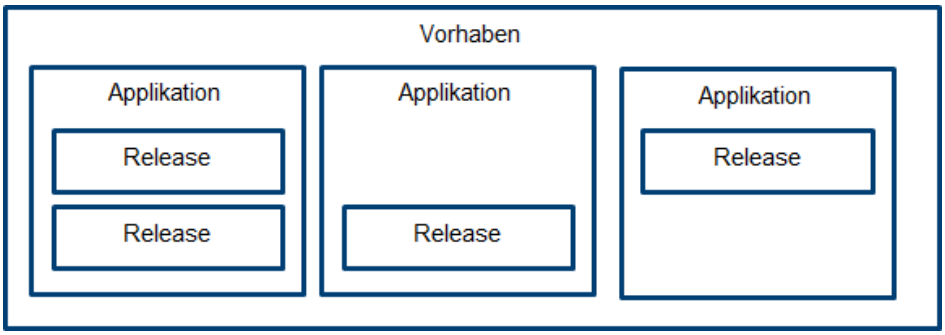

Abbildung 4 - Scope der Kontrolle festlegen: Vorhaben, Applikation oder Release

Diese Lösung adressiert die Natur der Vorhaben, für mehrere Teilapplikationen Releases einzuplanen, in dem möglichst wenige Kontrollen auf Releaseebene positioniert werden, und möglichst viele auf Applikations- und Vorhabenebene.

4 Methode

Die Umsetzung des Vorhabens wurde projekthaft durchgeführt. Hierzu wurde ein Projektleiter aus einer der bündelspezifischen Projektleitergruppen bereitgestellt. Die fachliche Projektleitung wurde vom Process Owner des *Release Managements* durchgeführt, da dort bisher die Pflege der SAC-Liste (zentrale Kontrollliste) angesiedelt war.

Im Wesentlichen wurde die Überarbeitung der Kontrollen in zwei Workshop-Reihen durchgeführt.

4.1 Workshop-Reihe 1: Klärung der Kontrollen

Mit jedem der vierundzwanzig betroffenen IT Prozesse wurden, um die Kontrollen des jeweiligen Prozesses zu klären, 1-3 Workshops durchgeführt und protokolliert. Dabei haben neben den Projektleitern und einer Projektassistenz jeweils der Process Owner des betroffenen IT Prozesses, sowie die Process Manager (typischerweise ein Vertreter pro Bündel, siehe Kapitel 2.1 Trägerorganisation) teilgenommen.

Ursprünglich wurde hierfür ein Workshop-Format (Metaplanwände, Karteikarten, usw.) definiert, welches sich aber nicht als praktikabel erwiesen hat. Schnell hat sich gezeigt, dass die Prozesse in unterschiedlichen Reifegraden gelebt wurden, so dass die Erfassung von Ergebnistypen und zugehörigen Kontrollen sehr heterogen verlief:

Für die Mehrzahl der Prozesse (insbesondere die ISO 20.000 relevanten Prozesse) konnten die Kontrollen bündelübergreifend innerhalb eines einzigen Termins genannt werden.

Für andere Prozesse starteten zunächst bündelübergreifende Diskussionen, wie der Prozess derzeit in den Bündeln etabliert ist. Als klarer positiver Seiteneffekt konnte für diese Prozesse der Beginn eines bündelübergreifenden Wissens- und Erfahrungsaustauschs verbucht werden.

Eines der Ziele war die Reduktion von Kontrollaufwand. Ein Hauptargument für die Process Owner zur Reduktion von Kontrollen war der Hinweis, dass sie über die entstehende Kontrolldatenbank in Zukunft sehr einfach nachjustieren können, falls ein Thema bei Produktivnahmen zu Herausforderungen führt. Vielfach konnte so ein risikoorientierter Ansatz mit unterschiedlichen Kontrolltiefen je Applikationstyp oder Projektszenario verhandelt werden.

4.2 Workshop-Reihe 2: Übergreifende Themen klären

Durch die Workshop-Reihe 1 wurden eine Reihe von Themen identifiziert, für welche sich unterschiedliche Prozess (in unterschiedlicher Art und Weise) verantwortlich fühlten. Da der Abbau von Redundanzen eines der Vorhabenziele war, wurde die Workshop-Reihe 2 durchgeführt. Dabei wurden die Process Owner der „rivalisierenden" Prozesse an den Tisch geholt. Dies waren zum Beispiel:

- Unterschiedliche Anforderungen an das DV-Konzept durch die Prozesse *Application and System Development* und *Availability and Capacity Management*. Die Anforderungen von *Availability and Capacity Management* bestand in der verbindlichen Abnahme aller DV-Konzepte durch die Capacity Experts, und war damit höher, als die Anforderungen des Prozesses *Application and System Development*.
- Klärung der Dokumentation von Configuration Items in der Konfigurationsmanagementdatenbank zwischen *Licence Management* und *Configuration Management*. Während *Licence Management* bereits für Entwicklungs-, Test- und Abnahmeumgebungen relevant ist, dokumentiert das *Configuration Management* den jeweils aktuellen Zustand der Produktionsumgebung.
- Unterschiedliche Vorgaben zum Berechtigungskonzept mussten zwischen *Identity and Access Management* und *IT Security Management* geklärt werden.
- Für den Ergebnistyp Schnittstellendokumentation machten die Prozesse *Interface Documentation, IT Architecture Management* und *IT Security Management* unterschiedliche Vorgaben.

4.3 Pflegeprozess definieren, abstimmen und etablieren

Für die erstmalig abgestimmte SAC-Liste wurde ein Pflegeprozess definiert. Es wurde zunächst eine Gesamtverantwortung für das neue Kontrollenmodell etabliert. Die einzelnen Ergebnistypen sowie Kontrollen, beziehungsweise Gütekriterien werden jedoch von den Prozessen verantwortet.

Der Pflegeprozess muss dabei mehrere Faktoren adressieren:

- Die Datenbank für das Kontrollenmodell soll als Anhang zur schriftlichen Ordnung, den Richtlinien, etabliert werden und unterliegt damit den gleichen Anforderungen.

- Es gibt 24 beteiligte Prozesse, die Ihre Ergebnistypen und Kontrollen in dem Kontrollenmodell führen sollen.
- Die Verantwortung für Kontrolle und Ergebnistypen liegt oft bei verschiedenen Prozessen.
- Zueinander redundante Inhalte von Kontrollen werden teils von verschiedenen Prozessen gefordert („Echte Redundanz“, siehe Kapitel 3.5).

Da das Rollenmodell für den Pflegeprozess mit den Prozesseigentümern vorgegeben ist, sind vor allem die Bedingungen für Veränderungen an den Kontrollen zu klären. Hierfür sind klare Ziele zu setzen und zu verfolgen:

1. Der Prozess soll transparent und unkompliziert sein.
2. Es gilt die Eigenverantwortung der jeweiligen Prozesse.
3. Veränderungen sollen ohne große Prüfung durch Dritte möglich sein.
4. Das Entstehen von Redundanzen soll vermieden werden.
5. Vorhandene Redundanzen sollen reduziert werden.

Die Ziele 4 und 5 werden im Rahmen der Gesamtverantwortung für das Kontrollenmodell verfolgt. Um bei größtmöglicher Eigenverantwortung dennoch eine zielgerichtete Entwicklung der Kontrollen zu unterstützen, sollen gemeinsam vereinbarten Prinzipien den Pflegeprozess leiten. Im Umfeld des Lean Managements haben sich hierbei die 5S-Arbeitsgestaltung und die daraus abgeleitete „5A-Methode“ etabliert, die hierzu herangezogen wird [Wi17]. Die Kernideen der fünf 5A-Prinzipien „Aussortieren“, „Aufräumen“, „Arbeitsplatzsauberkeit“, „Standardisieren“ und „Alles einhalten und verbessern“ dieser aus der Industrieproduktion stammenden Methode sollen auf den Pflegeprozess für das Kontrollenmodell übertragen werden:

1. Aussortieren

   Vorhandene Punkte, die nicht mehr benötigt werden, sollen regelmäßig geprüft, hinterfragt und aussortiert werden. Hierbei sollen nicht nur ganze Kontrollen, sondern auch einzelne Aspekte einer Kontrolle betrachtet werden. Wenn möglich, soll eine Aufwands- und Nutzenanalyse gemacht werden.

2. Aufräumen (Arbeitsmittel ergonomisch anordnen)

   Die vorhandenen Kontrollen sollen regelmäßig zusammen mit den anderen in Hinblick auf ihre Struktur geprüft werden. Die Kriterien sind dabei anhand des Konzepts vorgegeben: Die richtige Position in den Quality Gates sind zu prüfen, die Zuordnung des Scopes ebenso, wie die Relevanz für die einzelnen Szenarien in Bezug auf Abnahmekontrolle oder Checkpunkt. Hierzu kommt die übergreifende Dimension hinzu, dass auch Kontrollen und Ergebnistypen untereinander abgeglichen und betrachtet werden. Dabei sollen die inhaltlichen Abhängigkeiten zwischen den Ergebnistypen und Gütekriterien beachtet werden.

Letztlich soll auch die Toolzuordnung hierbei geprüft werden, um sicherzustellen, dass die Kontrollen in den richtigen Tools ausgeführt werden und dort wiederrum an der passenden Stelle stattfinden.

3. Arbeitsplatzsauberkeit

   Die einzelnen Kontrollen und Ergebnistypen müssen regelmäßig geprüft werden. Hierbei liegen die Formulierung und die Erläuterung von Ergebnistyp und Kontrollen im Fokus. Genauso sollen auch die einzelnen Dokumentationsorte und die Art der Dokumentation geprüft und aktualisiert werden. Im Rahmen dieser Prüfung sollte im Kontakt mit den Vorhaben Praxisbeispiele herangezogen werden und gemeinsam mit den Beteiligten inspiziert werden, um die Vorgaben inhaltlich zu prüfen.

4. Standardisieren

   Die Vorgaben und Kontrollen müssen laufend standardisiert werden, das heißt nach einheitlichen Kriterien dokumentiert und erläutert werden. Die Standardisierung kann dabei innerhalb eines Prozesses erfolgen, aber auch übergreifend.

5. Alle Punkte einhalten und verbessern

   Nicht unwesentlich ist, dass die definierten Ergebnistypen und Kontrollen tatsächlich eingehalten werden. Wird vereinzelt eine Übererfüllung oder Untererfüllung festgestellt, dann gilt es die Kontrollen an die Realität anzupassen, alternativ kann das Niveau entsprechend über Maßnahmen an die Kontrollen angepasst werden.

Über den Pflegeprozess sollen einzelne dieser Punkte selbstständig durch die Prozesse ausgeführt werden. Die übergreifenden Punkte werden zunächst periodisch durch einen Gesamtverantwortlichen gesteuert. Hierzu wird ein Maßnahmenkatalog etabliert, der regelmäßig durchgeführt dafür sorgt, dass einzelne Aspekte abgearbeitet werden.

4.4 Pilotierung

Für die Pilotierung werden jeweils zwei Projekte aus den Bündeln herangezogen, so dass die neue SAC-Liste mit acht Projekten verprobt wird. Nach sechs Monaten werden die Projektleiter und Betriebsverantwortlichen der betroffenen Systeme befragt. Die Pilotierung ist zum Zeitpunkt dieses Artikels noch nicht abgeschlossen. Anschließend zur Pilotierung wird eine Toolunterstützung angestrebt.

4.5 Lessons Learned

Im Laufe der Umsetzung haben wir einige Erkenntnisse gewonnen. Einmal wurde das Projekt von allen Beteiligten und Betroffenen gutgeheißen. Alle Process Owner haben bereitwillig mit uns zusammengearbeitet, nachdem wir Ihnen die Vorteile des neuen Verfahrens erläutert haben.

Die Prozessqualität ist natürlicherweise unterschiedlich. Die Diskussion mit den Process Ownern und Process Managern hat ergeben, dass Prozesse und Ergebnistypen besser ausgestaltet und verändert werden können, wenn es sich um Prozesse handelt, die über lange Jahre praxisnah etabliert sind. Jüngere Prozesse, oder Prozesse, die praxisfern entwickelt wurden, bedurften deutlich mehr Beratung und Unterstützung bei der Ausgestaltung der spezifischen Ergebnistypen und Gütekriterien. Eine anwendbare, aber nicht perfekte Lösung für einen Prozess ist besser als eine perfekte Lösung, die wegen des hohen administrativen Aufwands die Produktivität in Mitleidenschaft zieht. Diese altbekannte, immer wieder neu gewonnene Erkenntnis zeigt sich auch hier in zwei Facetten: Zum einen können sich die Prozesse in der Ausgestaltung ihrer Ergebnistypen verlieren und mit langen Gütekriterienlisten versehen, die weit über das leistbare hinausgehen, zum anderen kann auch das Modell der Quality Gates selbst eine Komplexität annehmen, die nicht mehr verständlich ist, und in der Praxis letztendlich scheitern muss.

5 Fazit

Die bisherige Lösung, die notwendigen Kontrollen im Rahmen der Service-Akzeptanzlisten einerseits auf ein Projekt und andererseits auf ein Release zu beziehen, hat sich als nicht praktikabel erwiesen. Denn dies führte dazu, dass ein Projekt je Release eine vollständige Kontrollliste zu bearbeiten hatte. Die Zusammenhänge sind in der Realität komplexer und erfordern eine Flexibilität, die sich mit starren Listen nicht abbilden lässt. Des Weiteren war bei der bisherigen Lösung in Frage gestellt, ob alle Kontrollen auf der Liste ausreichend aktuell und relevant waren. Aufgrund des fehlenden Bezugs zu den Prozessen war es nicht möglich, dies mit wenig Aufwand zu verifizieren.

Ein wesentliches Ergebnis der Überarbeitung der Kontrollen war zunächst, dass die meisten Kontrollen in der neuen Verantwortung der Prozesse inhaltlich fortbestehen. Es war dennoch erforderlich, den Kontrollen eine neue Struktur zu geben, die sie praxistauglich werden lassen. So sah die alte Lösung vor, dass dieselbe Kontrollliste je Applikation eines Projekts 160 Kontrollen enthält, die immer als Ganzes zu prüfen und zu bearbeiten waren. Die Beteiligten konnten zwar einzelne Kontrollen als nicht relevant einstufen, jedoch war es dafür notwendig, sie alle durchzugehen. Es blieb dabei nicht aus, dass auch für das Vorhaben nicht relevante Punkte bearbeitet wurden, genauso wurden aber auch relevante Punkte nicht bearbeitet – ein Qualitätsdilemma.

Anstatt 160 Kontrollen wurden für neue Applikationen 26 Ergebnistypen (nebst zugehöriger Gütekriterien) als abnahmerelevant identifiziert. Für normale Änderungen sind nur noch 14 Ergebnistypen abnahmerelevant, für Kleinständerungen nur noch 8. Damit konnten das ursprüngliche Projektziel einer Reduktion des Dokumentationsaufwands bei gleichbleibender Qualität erreicht werden. Für erfolgreichen produktiven Einsatz des neuen Kontrollsystems sind die Verbesserungsvorschläge der Pilotierungsphase einzuarbeiten und der Pflegeprozess aktiv zu etablieren.

Durch Umsetzung der im Kapitel 3 Aufbau des Lösungsbilds beschriebenen Maßnahmen und Einbindung aller betroffenen Stakeholder konnten der Dokumentationsaufwand sinnvoll reduziert werden. Die in Kapitel 3 beschriebene Struktur und die dazugehörigen Maß-

nahmen lassen sich sicher auf andere Unternehmen übertragen, falls dort auch eine heterogene Welt an Richtlinien und Kontrollen entstanden ist, oder um das Entstehen einer solchen zu vermeiden. Neben der praxistauglichen Struktur ist es essentiell, einen Pflegeprozess mit einem Process Owner aufzusetzen, der einen neuen Redundanzaufbau unterbindet.

Literaturverzeichnis

[Ba12] bafin.de, Rundschreiben 10/2012 (BA), https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1210_marisk_ba.html,Stand: 22.05.2017.

[Rö17] Röseler, R., https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Konsultation/2017/kon_0217_bankaufsichtliche_anforderungen_it_ba.html, Stand: 22.05.2017.

[Bu14] bundesfinanzministerium.de 2014, http://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf, Stand: 22.05.2017.

[Is17] Isselhorst, D.H., https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html, Stand: 22 05 2017.

[SJL16] Strüver, S.-C.; Jakobi, M.; Landua, M., Union Investment, https://www.heise.de/ct/artikel/Union-Investment-Integrationsplattform-auf-Basis-offener-Standards-221618.html, Stand: 22.05.2017.

[Wi17] Diverse, Wikipedia.de, https://de.wikipedia.org/wiki/5S, Stand: 18.01.2017.