

Lünendonk®-Whitepaper 2020

Sicheres Management: Vom Outsourcing zur Automatisierung

Compliance neu definieren
in der digitalen (R)Evolution



Eine Publikation der Lünendonk & Hossenfelder GmbH
in Zusammenarbeit mit



Inhalt

Vorwort	3	
Compliance neu definieren in der digitalen (R)Evolution	4	Vom SSC zur Automatisierung – Sicherheit im Wandel durch Digitalisierung 14
Die Evolution der Prozessoptimierung durch die Datenrevolution	6	Wie definieren wir Compliance in der Digitalisierung neu! 16
Stand der Automatisierung	8	Fazit und Zusammenfassung 21
Governance im Shared Service Center sowie bei der Prozessautomatisierung	10	Unternehmensporträts
Neue Anforderungen im Outsourcing	12	KPMG AG Wirtschaftsprüfungsgesellschaft 22 Lünendonk & Hossenfelder GmbH 23



Vorwort



Jonas Lünendonk,
Managing Director,
Lünendonk & Hossenfelder GmbH



Thomas Kern,
Partner Shared Service &
Outsourcing Assurance
KPMG AG
Wirtschaftsprüfungsgesellschaft

Liebe Leserin, lieber Leser,

die technologischen Möglichkeiten der zunehmenden Digitalisierung und Automatisierung von zahlreichen Verwaltungs- und Geschäftsprozessen bietet Unternehmen heute immense Vorteile. Effizientere und effektivere Prozesse erlauben die schnellere Bearbeitung von Serviceanfragen, eine Reduzierung von Fehlern bei standardisierten Tätigkeiten und die Möglichkeit, länderübergreifend Aufgaben zu bearbeiten. Ausführliche Gespräche und Studien zeigen, dass die Unternehmen es sich zum Ziel gesetzt haben, dieses Potenzial gerade in Bezug auf unternehmensbezogene Dienstleistungen intensiv zu erschließen. Standardisierung, Bündelung, Skalierung und Automatisierung lauten hier die Stichworte. Die Chancen, die sich den Unternehmen bieten, gilt es heute zu nutzen.

Aber Achtung: Mit der zunehmenden Vernetzung und Digitalisierung, der grenzüberschreitenden Bearbeitung von Unternehmensprozessen und dem Einsatz von Cloud-Plattformen steigt die Komplexität und damit auch das Risiko für Unternehmen. Denn bei der Digitalisierung erhöhen sich nicht nur die Chancen, sondern auch die Risiken!

Um auch unter diesen neuen Rahmenbedingungen zukünftig die Compliance sicherzustellen, sind CFO, Prüfungsausschuss und Aufsichtsrat dazu angehalten, diese neu entstehenden Risiken durch die Anpassung der internen Kontrollsysteme im Auge zu behalten und aktiv zu managen. Denn um verantwortungsvoll Chancen und Gefährdungspotenziale im Rahmen der Digitalisierung beurteilen und richtig managen zu können, muss die interne Steuerung und Kontrolle von Unternehmensrisiken entsprechend angepasst werden.

In diesem Whitepaper erfahren Sie, wie Unternehmen erste Schritte hin zu einem proaktiven und angemessenen Risikomanagement im Rahmen von Outsourcing, Shared Services und Digitalisierung bzw. Automatisierung gehen können.

Wir wünschen Ihnen eine aufschlussreiche Lektüre!

Jonas Lünendonk
Lünendonk & Hossenfelder

Thomas Kern
KPMG AG WPG





Compliance neu definieren in der digitalen (R)Evolution

Wir leben in innovativen Zeiten. Technik und Strukturen ändern sich in hohem Tempo. Das Wort „Revolution“ wird häufig genutzt. So sprechen wir beispielsweise von der „vierten industriellen Revolution“. Sie wurde ausgelöst durch die schnellen Innovationszyklen bei Vernetzung, Cloud sowie Analytics und künstlicher Intelligenz (KI). Diese Revolution wird allerdings speziell in Deutschland oft nur mit dem Thema Industrie 4.0 und der Produktion von Gütern „made in Germany“ in Verbindung gebracht. Das ist nicht falsch. Zweifelsohne verändern sich durch die Vernetzungs- und Anlysemöglichkeiten die industriellen Wertschöpfungsprozesse innerhalb und außerhalb der Fabriken. Aber diese Sichtweise erschließt nur einen Teil der Wahrheit.

Die weitaus größere „Revolution“ findet im Bereich der Dienstleistungen und damit im tertiären Sektor statt. Von deren umwälzenden Veränderungen sind, neben der Produktseite, vor allem die unternehmens-bezogenen Dienstleistungen und speziell die indirekten Bereiche wie Finance/Accounting, Human Resources, IT sowie Einkauf und Kundenservice betroffen. Die zunehmende Digitalisierung der früher oft papierbasierten Verwaltungsprozesse ermöglicht in vielen Abteilungen heute

mehr Prozesstransparenz, eine schnellere Identifikation von Effizienz- wie auch Automatisierungspotenzial und eine höhere Effektivität. Die Motivation zur verstärkten Digitalisierung dieser Unternehmensfunktionen ist daher eindeutig. Kosten sollen gesenkt, Effizienzpotenziale durch die Automatisierung gehoben und die Servicequalität und -verfügbarkeit verbessert werden.

Zahlreiche Studien der letzten Jahre zeigen, dass das Potenzial grundsätzlich erkannt wird – es umzusetzen fällt den Unternehmen allerdings aus unterschiedlichen Gründen schwer. Ganz wesentlich hierfür ist: In zahlreichen Unternehmen fehlen schlichtweg die Voraussetzungen für die intelligente Automatisierung von Dienstleistungsaufgaben. Das beginnt bei einer schlechten Stammdatenqualität und geht über eine oftmals heterogene und veraltete IT-Landschaft mit nicht vorhandenen Schnittstellen bis hin zu stark ausgeprägten Silostrukturen und Prozessschwächen. So wird in vielen Fällen eine bereichsübergreifende und damit horizontale Prozessbetrachtung und -optimierung im Sinne eines End-to-End-Ansatzes verhindert. Im Zeitalter der Digitalisierung ist diese übergreifende Betrachtung jedoch absolut notwendig.



Es überrascht daher nicht, dass nun zahlreiche Unternehmen angekündigt haben, ihre IT-Systeme und Business-Anwendungen zu vereinheitlichen und zu modernisieren, um Schnittstellen zu reduzieren und die Datenverfügbarkeit und -qualität zu verbessern. Gleichzeitig erfreut sich das Thema Agilität, also die flexible Form der Projektumsetzung, sehr großer Beliebtheit. Besonders Großunternehmen und Konzerne erhoffen sich dadurch, die abteilungsübergreifende Zusammenarbeit bei Digitalprojekten verbessern und beschleunigen zu können. Im Zuge dieser Entwicklung kommt der IT eine enorme Bedeutung zu. Sie spielt heute in nahezu allen Unternehmensbereichen eine zentrale Rolle, wenn es um die Unterstützung des Geschäfts geht – sowohl im Hinblick auf die Effizienz als auch auf die Effektivität.

Im dritten Quartal 2019 zeigte sich in Deutschland eine deutliche Abschwächung der konjunkturellen Entwicklung. Und auch in den kommenden Monaten ist damit zu rechnen, dass die dynamische wirtschaftliche Entwicklung der letzten zehn Jahre auf absehbare Zeit nachlassen wird. Zahlreiche Faktoren (u. a. Brexit, Handelsbarrieren etc.) führen derzeit zu einer Verunsicherung der Unternehmen. Infolgedessen werden die Budgets, die in den letzten Jahren stark in Richtung In-

novationsentwicklung, Wachstum und Digitalisierung flossen, nun kleiner und Themen rund um Effizienzsteigerung und Kostensenkung rücken auf der Agenda der Unternehmen wieder weiter nach oben.

Besonders die indirekten Bereiche stehen dabei verstärkt im Fokus. Für viele Unternehmen sind sie ein wichtiges strategisches Instrument, um durch Bündelung und Standardisierung von Aufgaben Effizienzpotenziale zu heben und die dadurch verfügbar gemachten Ressourcen auf komplexere Aufgaben auszurichten. Hinzu kommt, dass die Digitalisierung zahlreicher Verwaltungsprozesse in den letzten Jahren die Basis geschaffen hat, mithilfe digitaler Tools große Effizienzgewinne zu erzielen – sowohl durch die Automatisierung als auch durch die Abwicklung von Verwaltungsprozessen in Near- oder Offshore-Regionen. Allerdings sollte den Unternehmen bewusst sein: Bei aller Automatisierung und Digitalisierung muss die Sicherheit und Compliance der eingesetzten (IT-)Tools und Dienstleister gewährleistet sein. Denn die Skalierung der Bearbeitung und die Auslagerung von Aufgaben führen auch zu einer Skalierung der Risiken. In diesem Sinne gilt es für die Unternehmen, Voraussetzungen zu schaffen, damit Risiken frühzeitig erkannt, gemanagt und minimiert werden können.

Fehlende Voraussetzungen für die intelligente Automatisierung von Dienstleistungsaufgaben

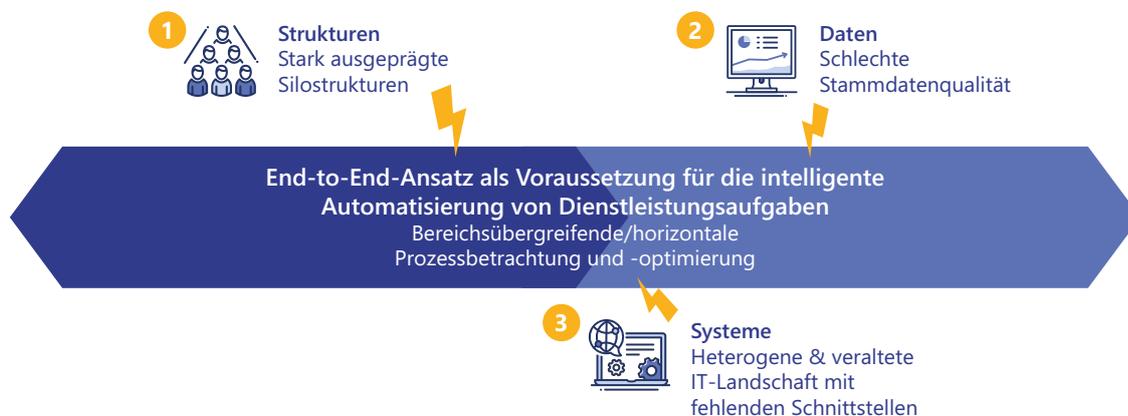


Abbildung 1: Herausforderungen bei der Automatisierung von administrativen Prozessen



SHARED SERVICES CENTER

Die Evolution der Prozessoptimierung durch die Datenrevolution

Um den aktuellen Stand der Automatisierung in unterschiedlichen Shared Service Centern (SSC) beurteilen zu können, wurden im Vorfeld dieser Publikation Sekundärquellen (u. a. aktuelle Studien) ausgewertet und neun ausführliche Expertengespräche mit Verantwortlichen von Shared-Service- und Outsourcing-Organisationen geführt. Die Gespräche haben gezeigt, dass die Unternehmen vor unterschiedlichen Herausforderungen stehen. Allerdings konnten auch einige Parallelen identifiziert werden, mit denen sich Unternehmen derzeit beschäftigen müssen.

Dies beginnt beispielweise mit der Tatsache, dass der demografische Wandel und damit die Verfügbarkeit von Fachkräften auch vor den SSC nicht haltmacht. Motivierte und verlässliche Mitarbeiter zu gewinnen wird zur zentralen Herausforderung. Darüber hinaus führt die Automatisierung von Teilaufgaben in der Verwaltung dazu, dass der ursprüngliche Gedanke eines rein transaktionalen SSC in den Hintergrund, Ansätze im Sinne eines Center of Excellence dagegen in den Vordergrund rücken. Entsprechend gestalten sich die Aufgaben der Mitarbeiter im SSC immer komplexer und damit anspruchsvoller, was wiederum Einfluss auf

die Rekrutierung qualifizierter Fachkräfte hat. Zusätzlich fehlen den SSC oftmals die Fachkräfte, um die eigene Automatisierung schnell und erfolgreich vorantreiben zu können. Die Unternehmen müssen hier reagieren und die Investitionen in die Automatisierung von Shared Service Units erhöhen. Nur wenn entsprechende Budgets zur Verfügung stehen, kann in der Folge das Automatisierungspotenzial auch gehoben werden, um Prozesse auf der Basis neuer Technologien erfolgreich in der Organisation zu verankern.

Herausforderungen in der Praxis



Abbildung 2: Praxisherausforderungen

Die Gespräche mit den Entscheidern und Unternehmenspraktikern machen deutlich, dass Technologien wie beispielsweise RPA (Robotic Process Automation) theoretisch großes Effizienzpotenzial aufweisen; dieses jedoch zu heben und aus einem identifizierten Use Case einen erfolgreichen Business Case zu machen fällt vielen Unternehmen schwer. Der Grund: Oftmals fehlt die notwendige Datenqualität, um manuelle, repetitive Aufgaben mit großem Volumen buchungskreisübergreifend skalierbar zu standardisieren. Darüber hinaus handelt es sich bei Automatisierungslösungen um Software-Tools, die auf der Basis eines transparenten und nachvollziehbaren Governance-bezogenen Framework entwickelt, getestet und betrieben werden sollten. Die dafür erforderliche Kompetenz ist in den Unternehmen und den einzelnen Fachbereichen jedoch häufig noch nicht vorhanden.

Vor diesem Hintergrund waren die befragten Experten der Meinung, dass gerade dem SSC in Unternehmen die Rolle des Automatisierungsexperten zukomme – bringt das SSC doch zahlreiche Voraussetzungen mit, die es

ermöglichen, Automatisierungslösungen nicht nur zu skalieren, sondern auch compliant und auf der Basis eines einheitlichen Vorgehensmodells zu entwickeln. Die hohe Zahl standardisierter Prozesse, die große Prozesskompetenz sowie die oftmals weit übergreifende Prozessverantwortung und reduzierte Schnittstellen im Sinne eines End-to-End-Ansatzes machen die SSC zu prädestinierten Unternehmenseinheiten, um Automatisierung nicht nur zu testen, sondern auch wirtschaftlich zu skalieren. Vor diesem Hintergrund kommt diesen Einheiten eine besondere Bedeutung zu.

Nur spiegelt sich diese Wertigkeit derzeit nicht in den Budgets wider. SSC werden oft als reine Cost Centers betrachtet. Daher fehlen ihnen teilweise die Budgets, um weitere und neue Ressourcen für die Entwicklung von Automatisierungslösungen bereitstellen zu können. Der zunehmende Einsatz von RPA und KI bietet ihnen jedoch die Chance, sich noch stärker als bisher auf Effizienz für ihre Standardaufgaben zu konzentrieren und damit Freiräume zu schaffen, um sich zusätzlich in Richtung eines Kompetenzzentrums der Automatisierung zu entwickeln.

Shared Services als Digitalisierungsexperten



Abbildung 3: Gute Voraussetzungen im SSC für die Automatisierung





Stand der Automatisierung

Bei der Frage, wo Automatisierungslösungen bereits zum Einsatz kommen, fallen die Aussagen recht eindeutig aus: Nur wenige Unternehmen können bereits auf eine umfassende Automatisierungserfahrung blicken. Zahlreiche Unternehmen stehen noch am Anfang und haben bis dato erst einzelne Aktivitäten mittels RPA automatisiert. Teilweise erklären die Gesprächspartner auch, zur Sammlung von Erfahrungen einzelne Use Cases umgesetzt zu haben, dass der Business Case jedoch nicht erreicht werden konnte. In vielen Fällen experimentieren die Unternehmen derzeit noch mit RPA-Lösungen.

Die Gespräche zeigen allerdings auch, dass Themen wie Compliance, Verständlichkeit und Nachvollziehbarkeit eine immer bedeutendere Rolle spielen. Schließlich sind zahlreiche Finance-, Accounting-, HR- und IT-Prozesse von diesen Veränderungen betroffen und eine verlässliche Ausführung ist eklatant wichtig. Dies gilt besonders vor dem Hintergrund, dass die automatisierte Bearbeitung von Aufgaben für den Wirtschaftsprüfer und für weitere Prüfinstanzen transparent und nachvollziehbar sein muss.

Hier beginnt aber für viele Unternehmen bereits die Schwierigkeit beim Einsatz von KI-Lösungen. Oftmals fehlt durch den Einsatz bestimmter Algorithmen (u. a.

neuronale Netze) die Nachvollziehbarkeit und Erklärbarkeit. Hinzu kommt, dass die genutzten Trainingsdaten ebenfalls einen großen Einfluss auf die spätere Ergebnisqualität haben und zudem erst einmal zu einer ausreichend sicheren Funktionalität des Algorithmus führen müssen. Dieser Herausforderung sind sich die Unternehmen durchaus bewusst. Daher werden wirkliche KI-Lösungen derzeit nur mit großer Zurückhaltung eingesetzt, wenn es um die tatsächliche Bearbeitung von Aufgaben geht.

Eine viel größere Rolle spielen KI-Lösungen momentan bei der Entscheidungsvorbereitung (u. a. Anomalie-Erkennung, Qualitätssicherung) und bei der Vorstrukturierung von Lösungen (z. B. „next best offer“, Identifikation von Potenzialkunden, Buchungsvorschläge), wobei aber der Mensch die finale Entscheidung trifft. Dieses sinnvolle Zusammenwirken von Mensch und KI-Lösung wird daher wohl in absehbarer Zeit der Haupteinsatzbereich für reine KI-Lösungen sein. Das zeigten auch die Expertengespräche. Deshalb wird im Folgenden der Schwerpunkt stärker auf Robotic Process Automation gelegt.

Warum stellt sich im Vergleich zu den Herausforderungen rund um KI die Situation bei RPA-Lösungen deutlich anders dar? Die klare Antwort: Da RPA-Anwendungen



Unternehmen sind oft noch in der Testphase von RPA- und KI-Lösungen



Vor- und Nachteile von Robotic Process Automation (RPA)



Nachvollziehbarkeit & Verständlichkeit



Geringe Flexibilität bei Ausnahmen, Veränderungen oder heterogener IT-Landschaft



Die meisten aktuellen KI-Lösungen nehmen eine große Rolle bei der Entscheidungs-vorbereitung und Vorstrukturierung von Lösungen ein, wobei der Mensch anschließend die finale Entscheidung trifft.

Abbildung 4: Unternehmen experimentieren derzeit oft nur mit Automatisierungslösungen

strukturierte Aufgaben anhand klar definierter Kriterien und Abläufe umsetzen, ist deren Nachvollziehbarkeit hoch. Dies geht allerdings zulasten der Flexibilität. So benötigen RPA-Anwendungen stabile Prozesse und Anwendungsoberflächen mit wenigen Ausnahmen und geringen Veränderungen im Zeitverlauf, die auf klar strukturierten und homogenisierten Daten basieren. Sobald die Zahl der Ausnahmen innerhalb von Prozessen zu hoch ist oder die heterogene IT-Landschaft die breite Anwendbarkeit reduziert, lohnt sich der Einsatz oft nicht mehr. Allerdings nutzen einzelne Unternehmen RPA-Lösungen auch, um Schnittstellen aufgrund der heterogenen IT-Landschaft gezielt zu überbrücken. Dies sind jedoch zumeist Übergangslösungen, die mit der Standardisierung der IT-Systeme abnehmen.

Darüber hinaus machen die Expertengespräche deutlich, dass die Identifikation von RPA-Prozessen teilweise nur schwer gelingt. Als Daumenregel wurde beispielsweise genannt: Der RPA-Einsatz lohnt sich, wenn mindestens 0,5 FTE (Full Time Equivalents) pro Tag ersetzt werden können. In der heutigen Zeit stellt sich allerdings die Frage, wie hoch die Zahl von Tätigkeiten ist, die in dieser Frequenz einen Mitarbeiter in gleicher Form beschäftigen. Zudem lassen sich oft nur einzelne Aktivitäten und ggf. Teilprozesse automatisieren, die jedoch insgesamt einen derartigen

FTE-Effekt erzielen können. Wenn die genannten Voraussetzungen gegeben sind, kann RPA daher sehr positive Auswirkungen auf die Organisation und die Kostenstruktur entfalten.

Konkret versprechen sich die Unternehmen von RPA und anderen Optionen nicht nur Effizienz- und Kostenvorteile, sondern auch die Steigerung der Qualität bei der Aufgabenbearbeitung. Denn Menschen neigen insbesondere bei der Bearbeitung monotoner Aufgaben zu Fehlern, RPA-Lösungen können jedoch eine hohe Qualität sicherstellen. Gleichzeitig wurde deutlich, dass Effizienzgewinne nicht zwangsläufig zur Reduzierung der Mitarbeiterzahl führen. Vielmehr möchten die Unternehmen die Mitarbeiter für interessantere und höherwertigere Dienstleistungen qualifizieren und einsetzen. Gerade in Zeiten des demografischen Wandels sollen Fachkräfte mit Prozess-Know-how gehalten werden. Beispiel: Es ist für einen Mitarbeiter deutlich spannender, nicht täglich den gleichen Report für bestimmte Kennzahlen zu erstellen, sondern vielmehr die Empfänger auf Abweichungen und mögliche Ursachen hinzuweisen. Daher sollen RPA-Tools in erster Linie in Finance (u. a. Informationsbereitstellung), Accounting (Pay-Prozesse), HR (u. a. Chatbots), IT (First-Level-Support) sowie im operativen Einkauf zum Einsatz kommen.





Governance im Shared Service Center und bei der Prozessautomatisierung

Die Expertengespräche zeigen: Für Unternehmen ist das SSC die Chance, betrieblich erforderliche beziehungsweise vorgeschriebene Nebentätigkeiten stärker zu professionalisieren und auf dieser Basis anschließend automatisieren zu können. Denn den einzelnen Fachabteilungen fehlen oft geeignete, skalierbare Prozesse und Aktivitäten mit einem angemessenen Automatisierungspotenzial und gleichzeitig einheitlicher Datenqualität. Darüber hinaus bietet ein SSC die Möglichkeit, sehr verteilt stattfindende Prozesse im Unternehmen wieder stärker an einer Stelle zu bündeln und zusammenzuführen. Dadurch steigt der Gesamtüberblick, und Ineffizienzen in den Prozessen lassen sich schneller aufdecken. Außerdem sinkt die Zahl der Schnittstellen, und Veränderungen können schneller End to End adaptiert werden.

Bei allen gebotenen Chancen der neuen digitalen und organisatorischen Möglichkeiten müssen die Verantwortlichen aber stets anhand wirksamer Kontrollen sicherstellen, dass Risiken für das Unternehmen frühzeitig erkannt und abgestellt werden. Gerade wenn Aufgaben von internen Servicedienstleistern wie dem SSC übernommen werden, gilt es, die durch die Entkopplung entstehenden Risiken zu organisieren und zu managen, ins-

besondere weil die Verantwortung bei der auslagernden Einheit verbleibt. Der Aufbau eines operativen internen Kontrollsystems ist in diesem Zusammenhang zwingend notwendig. Ziel dieses internen Kontrollsystems (kurz: IKS) ist es, Fehler und Risiken frühzeitig zu erkennen, zu korrigieren und dauerhaft abzustellen. Dabei werden die Prozesse und deren Risiken im Hinblick auf unterschiedliche Dimensionen (u. a. finanzieller Schaden, operative Risiken, Betrugsrisiken etc.) bewertet und dokumentiert (z. B. Flow-Charts, Prozessbeschreibungen etc.). Allerdings genügt es hier nicht, eine Dokumentation vorlegen zu können. Eine angemessene Compliance beinhaltet darüber hinaus eine regelmäßige und individuelle Prüfung von IKS und Key Performance Indicators (KPIs) anhand vorgegebener Standards (beispielsweise ISAE 3402, SOC II oder BSI C/5) durch das Unternehmen wie auch durch den beauftragten Wirtschaftsprüfer. Für diese Notwendigkeiten müssen die Kontrollen klar definiert und die Mitarbeiterinnen und Mitarbeiter sensibilisiert und geschult werden. Letztendlich müssen die Unternehmen aus den Prüfergebnissen konkrete Maßnahmen und Handlungen ableiten, um die IKS stets auf dem aktuellen Stand zu halten. Dieses strukturierte Vorgehen sowie die eindeutige Nachvollziehbarkeit von Aktivitä-



ten und Prozessen sind auch bei der Automatisierung von Aufgaben mittels Automatisierungstechnologien (RPA und andere) unabdingbar. Gleichzeitig sind die Verantwortlichkeiten für den Betrieb solcher Lösungen klar zu regeln, sodass die Abteilungen nachvollziehbar Verantwortung für die betriebene Lösung übernehmen können und der Schadensfall möglichst vermieden wird.

SICHERHEIT BEIM EINSATZ VON AUTOMATISIERUNGSTECHNOLOGIEN

Automatisierungstechnologien spielen gerade bei Prozessen mit hohem Volumen und standardisierten Systemen alle ihre Vorteile aus. Das bedeutet, dass die Skalierung standardisierter Bearbeitungsprozesse durch RPA-Technologien oftmals sehr einfach möglich ist. Allerdings ist zu beachten: Mit diesem Potenzial skaliert auch das Risiko. Sollten vorsätzlich oder versehentlich falsche Prozesse ausgeführt werden, kann für Unternehmen großer Schaden entstehen, zum Beispiel durch die Anlage falscher Lieferanten und Rechnungen. Aber nicht nur im Prozess selbst sind Manipulationen oder Fehler möglich, bereits bei der Entwicklung und Projektumsetzung gilt es, die üblichen Vorgehensweisen und Qualitätsstrategien eines Software-Projekts zu beachten. Außerdem müssen die IT-Systeme, auf denen die RPA-Bots installiert sind, den üblichen IT-Sicherheitsauflagen entsprechen, um Betrug, Datenverlust oder Datenmanipulationen zu verhindern.

Zwar befinden sich viele Unternehmen noch am Anfang ihrer Automatisierungsreise, sie sollten allerdings schon bei der Entwicklung, beim Test und beim anschließenden Betrieb von RPA-Lösungen darauf achten, dass diese Reise anhand eines konkret vereinbarten Rahmenwerks und mithilfe von standardisierten Kontrollen und Checklisten stattfindet. In der Entwicklung stellen angemessene IT-Change-Management-Prozesse und eine klare Rollenteilung bereits die Compliance und die Nachvollziehbarkeit der Automatisierungslösungen sicher. Darüber hinaus erfordern die laufenden RPA-Prozesse stets ein geeignetes KPI-Monitoring bzw. regelmäßige Prüfungen, um Abweichungen oder Anomalien im Betrieb frühzeitig erkennen und abstellen zu können. Nur wenn Unternehmen bereits heute diese Basis schaffen, können die RPA-Prozesse

künftig als vertrauenswürdig eingestuft und damit vom Prüfer abgenommen werden. Ist das nicht der Fall, wird dies zwangsläufig zu Risiken führen, die im Rahmen des IKS auffallen müssen, da sie erheblich sein können.

Zusätzlich müssen die Unternehmen sicherstellen, dass RPA-Anwendungen auf einer modularen Programmierung fußen. Ansonsten beeinflussen Updates einzelner Anwendungen (u. a. von Office-Programmen) die Funktionsfähigkeit zahlreicher RPA-Prozesse und ziehen damit manuelle Änderungen in diesen Prozessen nach sich. An dieser Stelle zeigt sich bereits, dass RPA- und andere Automatisierungstechnologien nicht unvorbereitet und zu schnell eingeführt werden sollten, sondern einer stringenten Vorgehensweise bei der Entwicklung folgen müssen.

Damit Automatisierungslösungen also erfolgreich und nachhaltig entwickelt, eingeführt und betrieben werden können, sind in den Unternehmen eindeutige Voraussetzungen dafür zu schaffen – sowohl im Hinblick auf technologische, auf prozessuale als auch auf organisatorische Anforderungen. Dies beginnt beispielsweise mit dem Aufbau bereichsübergreifender Teams, die Automatisierungsvorhaben fachlich und technisch anhand eines konkreten Framework auswählen, begleiten und umsetzen können. Fester Bestandteil dieser Teams sollten Prozessexperten sein, die frühzeitig in die Entwicklung eingebunden werden, um Sonderfälle und Ausnahmen rechtzeitig erkennen und diskutieren zu können. Und selbstverständlich muss die IT-Abteilung als Partner mit an Bord sein, um eine sichere Infrastruktur für Automatisierungslösungen bereitstellen zu können. Eine weitere zwingende Voraussetzung: Die Unternehmen müssen ihre Hausaufgaben im Bereich der Stammdaten und der Modernisierung von Legacy-Anwendungen umsetzen. Denn, so machten die befragten Experten deutlich, nur wenn verlässliche Daten und moderne und schnittstellenoffene Anwendungen im Einsatz sind, können Automatisierungsvorhaben tatsächlich schnell zu Verbesserungen führen. Teilweise liefern die neuen ERP-Systeme sogar Automatisierungslösungen mit, die sich für standardisierte branchenspezifische Prozesse schnell und einfach aus dem Standard übernehmen lassen.





Neue Anforderungen im Outsourcing

Neben der Bündelung und Standardisierung von Aufgaben innerhalb von Unternehmen spielt nach wie vor die Vergabe einzelner Aufgaben oder ganzer Prozesse für die Unternehmen eine wichtige Rolle. Entsprechend lohnt sich ein Blick auf die Trends und Entwicklungen im Outsourcing, das sich als Handlungsoption in Deutschland Ende der 80er-Jahre des letzten Jahrhunderts zu etablieren begonnen hat.

Outsourcing funktioniert stets dann gut, wenn funktionierende Teil- oder Gesamtprozesse an externe Service-Partner temporär oder dauerhaft übertragen werden können. Außerdem ist ein Agieren auf Augenhöhe – zum Beispiel ähnliche Größe von Kunde und Dienstleister – sinnvoll. Beim Outsourcing hat sich die jahrzehntelange Praxis zwischen Unternehmen und Dienstleistern bewährt und wurde stetig professionalisiert. Jedoch haben sich hier die Rahmenbedingungen in den letzten Jahren deutlich geändert. Die Fülle

regulatorischer Anforderungen – schließlich verwalten Dienstleister unternehmensinterne, vertrauliche und personenbezogene Daten auf ihren Systemen – hat erheblich zugenommen. Mit der europäischen Datenschutz-Grundverordnung (DSGVO) wurde hier eine neue Belastungsspitze erreicht. Zusätzlich nehmen mit fortschreitender Cyber-Wirtschaft auch die Gefahren zu. Die Netze und Datenspeicher zahlreicher Unternehmen und Organisationen jeder Provenienz werden täglich vielfach von außen angegriffen. Cyber Security hat daher ebenfalls massiv an Bedeutung gewonnen. Outsourcing-Anbieter müssen hier laufend erhebliche Investitionen tätigen, um ihre Kunden zu schützen und ihren Security-Pflichten nachzukommen.

Zudem reicht es heute nicht mehr, nur Standard- und Basisleistungen anzubieten. So wird von Outsourcing-Dienstleistern Fach- und Branchenkompetenz verlangt, um beispielsweise beim Thema Financial Services den



hohen regulatorischen Anforderungen gerecht zu werden, die an ihre Kunden und damit auch an sie gestellt werden. Zudem müssen sie Guidelines und Auditierungen vorweisen, um überhaupt auftragsfähig agieren zu können. Die den ausgelagerten Prozessen und Aktivitäten übergeordneten Governance-Strukturen müssen heute durch unabhängige Prüfer, beispielsweise Wirtschaftsprüfer, bestätigt werden.

Unternehmen müssen sich zudem heute darüber im Klaren sein, dass durch den Einsatz von Cloud-Diensten beim Outsourcing-Partner neue Risiken entstehen. So setzen Outsourcing-Dienstleister ebenfalls darauf, zahlreiche Aufgaben der Kunden automatisiert abwickeln zu können. Dies geschieht häufig durch den Einsatz von Automatisierungslösungen, die große Cloud- oder RPA-Software-Unternehmen den Outsourcing-Unternehmen zur Verfügung stellen. Sollte es bei einem dieser Anbieter zu einer Datenpanne kommen oder personenbezogene Daten in den falschen Ländern verarbeitet werden (z. B. außerhalb der EU), ist das Auftraggeberunternehmen gegenüber seinen Kunden und Lieferanten in der Verantwortung. Diese Risiken gilt es bereits in der Vertragsphase im Blick zu haben und im laufenden Betrieb zu überwachen, sodass die Risiken trotz Outsourcing-Partner handhabbar bleiben.

Für ein erfolgreiches Outsourcing zeichnet jedoch nicht nur der externe Dienstleister verantwortlich. Eine klare Definition, welche SLAs (Service Level Agreements) und welche Margen den Rahmen der Zusammenarbeit bilden, ist zwingend erforderlich. Hinzu kommt, dass die Outsourcing-Mitarbeiter wie eigene Mitarbeiter betrachtet und gemanagt werden sollten, um Verständnis, Nachvollziehbarkeit und Kommunikationsqualität als Plattform erfolgreicher Zusammenarbeit zu sichern. Nicht zuletzt in der Erörterung, was outgesourct werden sollte und wie, erschließt sich Unternehmen häufig eine erhöhte Klarheit über die zentralen Prozesse und deren jeweilige

Relevanz für eine interne oder externe Bearbeitung. Mit Outsourcing gewinnen Unternehmen zum einen Kostenvorteile, zum anderen profitieren sie vom Know-how – Branche, Technik, Prozess, Best Practices – des Dienstleisters, der seine Erfahrungen aus vielfältigen Service-Situationen und mit zahlreichen Kunden einbringen kann. Im Umkehrschluss heißt das jedoch auch, dass Aufgaben dauerhaft abgegeben werden und damit mittel- oder langfristig eine Know-how-Verlagerung stattfindet. Dieses Risiko steigt noch, wenn es keine oder nur noch wenige Alternativen zum ausgewählten Dienstleister gibt, sodass sich Zwänge ergeben. Sinnvoll ist es, wie bereits erwähnt, einen Partner zu wählen, mit dem das Kräfteverhältnis stimmt, um nicht der „kleine Kunde“ neben vielen großen oder der „Großkunde“ neben wenigen anderen zu sein. Das Management der Abhängigkeiten ist ebenso wichtig wie die kontinuierliche Kontrolle der SLAs und der Performance. Darüber hinaus fordert Outsourcing insbesondere dann interne Ressourcen, wenn ein Unternehmen grenzüberschreitend agiert und international unterschiedliche Prozesse bewältigen muss. Zusätzlich müssen die lokal Verantwortlichen des Auftraggeberunternehmens durch regelmäßige Reviews sicherstellen, dass die vereinbarten Vorgehensweisen im laufenden Betrieb eingehalten werden.

Es würde an dieser Stelle zu weit führen, nun im Detail die Vor- und Nachteile von Outsourcing versus SSC darzustellen. Deutlich ist jedoch, dass beide Optionen – insbesondere vor dem Hintergrund der Chancen und Anforderungen der Digitalisierung – nützliche und sinnvolle Wege eröffnen, um die wichtigen Unternehmensaufgaben „hinter dem Vorhang“ effizient und erfolgreich zu bewältigen. Wenn die Compliance-Anforderungen im Blick behalten und die Risiken kontinuierlich geprüft, evaluiert und gegebenenfalls Maßnahmen zur Verbesserung abgeleitet werden, lassen sich die Potenziale der „digitalen (R)Evolution“ bei Tertiärprozessen nachhaltig erschließen.



Vom SSC zur Automatisierung – Sicherheit im Wandel durch Digitalisierung



Thomas Kern,
Partner Audit
Shared Service & Outsourcing Assurance
KPMG AG
Wirtschaftsprüfungsgesellschaft



Roxana Meschke,
Partner Audit
Compliance Governance Services
KPMG AG
Wirtschaftsprüfungsgesellschaft

RISIKEN IN DEN PROZESSUALEN ELEMENTEN DER DIGITALISIERUNG

In den vergangenen 20 Jahren waren das SSC und der BPO-Provider (Business Process Outsourcing) ein zentrales Mittel zum Sparen von Kosten und zur Optimierung von Prozessen. Diese Rolle kommt heute vermehrt der Digitalisierung und Automatisierung zu. Die Digitalisierungstools (D-Tools), RPA, Machine Learning (ML)¹ und KI werten – bei kontinuierlich sinkenden Kosten – Prozesse und Systeme mit weiteren Leistungsmerkmalen auf.

Auffallend ist, dass viele Unternehmen nicht nur in ihrem SSC in den letzten Jahren „Speck“ in Form von mehr und mehr ERP-System angesetzt haben. Die Prozesse werden durch fortschreitende Modularisierung und diversifizierte Arbeitsteilung immer weiter gesplittet und auf mehr Ebenen und damit Sub-Unternehmen ausgelagert. Bei steigenden Anforderungen an IT-System-Prüfungen und die Governance führt dies zu erhöhten Risiken und Kosten im Erstellungs-, Überwachungs- und Prüfungsprozess. Neben der Vielzahl von Systemen kumulieren sich Risiken u. a. bei der Modularisierung, den Systemschnittstellen, den mannigfaltigen Zugriffsrechten und der umfangreichen Wartung der vielen Systeme und Prozessvarianzen.

Diese Faktoren und die immer strengeren Anforderungen der Prüferaufsichten verlangen nach einem neuen Level der Zusammenarbeit von Prüfer und Unternehmer: „Sicherheit in Outsourcing und Digitalisierung“

müssen Cheftemen in Prüfungsausschüssen (PA) werden, um auch als Aufsichtsrat (AR) seinen Pflichten nach § 107 (3) AktG (u. a. Überwachung der Wirksamkeit interner Kontrollsysteme) angemessen nachzukommen.

PRÜFUNG BEI DER IMPLEMENTIERUNG VON SSC/ BPO UND DIGITALISIERUNG

Es ist heute noch sinnvoller als früher, den Prüfer (oder aus Unabhängigkeitsgründen „einen Prüfer“, der nicht der aktuelle Abschlussprüfer ist) von Anfang an als Berater in die Einrichtung von Outsourcing und Digitalisierungsmaßnahmen zu involvieren. Ein mit den Themen der Digitalisierung vertrauter Prüfer ist in der Lage, das Unternehmen intensiv und proaktiv zu unterstützen, um spätere Risiken von vornherein zu evaluieren, soweit möglich zu vermeiden bzw. angemessen zu reduzieren. Der Prüfer kann mittels Datenanalyse oder Process Mining die Ist-Aufnahme des Prozesses unterstützen und die Harmonisierung mit seinem Prozess- und Branchen-Know-how optimieren. Diversifizierte Prozesse und eine Vielzahl von ERP-Systemen werden die Kosten und Risiken im SSC stetig erhöhen und sollten daher frühzeitig auch unter dem Gesichtspunkt der Compliance diskutiert werden. Für die Sicherheit des IT-Umfeldes sind die zusätzlichen Risiken im SSC-/BPO-Umfeld (z. B. Systemzugänge oder Berechtigungskonzepte) immer frühzeitig aufzuzeigen.

Sobald Geschäftsbereiche und Prozesse für das SSC feststehen, kann ein prüfungserfahrener Berater zusam-

¹ Für Zwecke dieses Whitepapers definieren wir Machine Learning als lernende Algorithmen, die beispielsweise durch Labeling aus Unmengen von Daten Regeln und Klassifizierungen vornehmen – also auf der Ebene der Datenstruktur aktiv sind, während künstliche Intelligenz auf dem nächsthöheren Level anhand dieser strukturierten Daten dann Schlussfolgerungen (beispielsweise für die Zukunft) zieht bzw. zu ziehen lernt.

men mit dem Unternehmen an einer einheitlichen Prozessbeschreibung (End to End) arbeiten, den (einheitlichen) Activity-Split definieren und die dazu notwendige Risiko-Kontroll-Matrix (RKM) ableiten. Ziel ist es, den Prozess auch weiterhin mittels eines angemessenen IKS abzusichern. Insbesondere das IKS ist eine Kernkomponente, die nicht unterschätzt werden sollte:

1. Der Prüfer verfügt über umfangreiche Erfahrungen zu IKS aufgrund seiner eigenen Tätigkeit.
2. Der in Digitalisierung erfahrene Prüfer kann jederzeit die effektivsten und effizientesten Kontrollen identifizieren, um potenziellen Risiken optimal zu begegnen.

Dieses IKS bildet zukünftig die Grundlage für die Jahresabschlussprüfung. Eine Abschlussprüfung kann nur dann effizient abgewickelt werden, wenn sich der Abschlussprüfer hinsichtlich SSC/BPO und Digitalisierung auf ein einheitliches² IKS verlassen kann. Zur Messung von Performance, Effizienz und Effektivität des SSC sind KPIs festzulegen, die üblicherweise im SLA vereinbart werden und unter betriebswirtschaftlicher Sicht zu beurteilen sind. Diese KPIs sollten mehr und mehr einen qualitativen und dynamischen Charakter erhalten. Hier kann der Berater mit seinen digitalen Tools (z. B. einem D&A Dashboard) effizient beitragen. Die KPIs sind entlang des Prozesses so anzulegen, dass sie (a) keine Fehlanreize geben und (b) jederzeit messbar sind. Eine

regelmäßige Überwachung und klare Konsequenzen bei Nichteinhaltung sollten in diesem Zusammenhang genauso selbstverständlich sein wie die regelmäßige Überprüfung des KPI-Systems insgesamt auf der Basis des aktualisierten Digitalisierungsniveaus. Die Prüfung des IKS erfolgt entweder durch den Abschlussprüfer selbst oder mittels einer Prüfung nach dem internationalen Standard ISAE 3402 „Assurance Report on Controls at a Service Organisation“ durch speziell geschulte und erfahrene IKS-Prüfer.

Neben den SSC/BPO-Ansätzen müssen Mandant und Abschlussprüfer auch die Effekte der Digitalisierung berücksichtigen. Das bedeutet, dass beispielsweise RPA, ML und KI, die in Prozessen aktive Kontrollen durchführen, gleichermaßen zu berücksichtigen sind wie Prozessautomatisierungen und Chancen neuer Technologien wie beispielsweise das neue ERP-System SAP S/4HANA. Bei einem standardisierten Prozess sollte nach erfolgreicher Prüfung der Prüfschritte 1 und 2 die verbleibende Prozessprüfung – vor allem der Prozessschritte 3.2 und 3.3 – durchaus geringer ausfallen als bisher (siehe Abbildung 5). Dies macht deutlich, wie wichtig nicht nur die Harmonisierung, sondern auch die Standardisierung der Prozesse und IT-Systeme ist.

Wie wirkt sich die Digitalisierung des Mandanten konkret auf die Prüfung aus und wie wird die Sicherheit gewährleistet?

Die drei Stufen der aktuellen Prüfung im digitalisierten und von SSC/BPO geprägten Umfeld

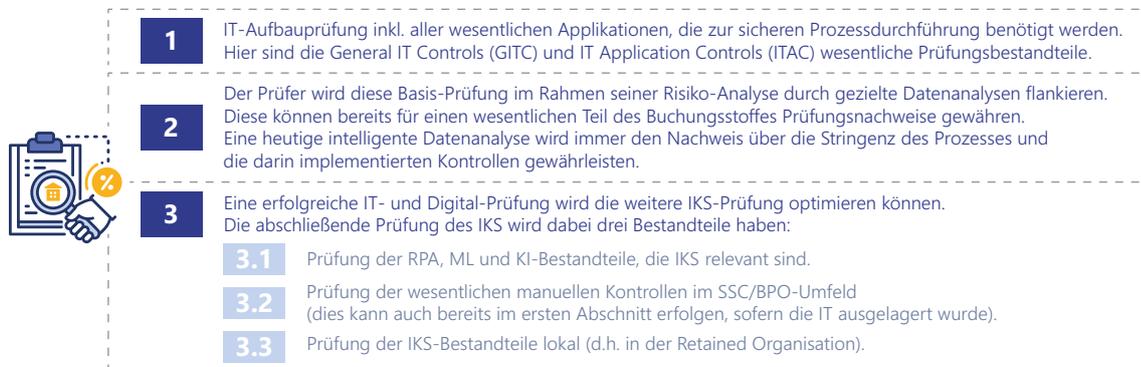


Abbildung 5: Der 3-Stufen-Prozess der aktuellen Prüfung im digitalisierten und von SSC/BPO geprägten Umfeld

² KPMG führt jährlich bei weit über 1.500 Prüfungen detaillierte Datenanalysen durch und kann diese sowie das noch umfangreiche Prozess-Know-how jederzeit benchmarken.



Wie definieren wir Compliance in der Digitalisierung neu

DIGITALISIERUNG ERSETZT OUTSOURCING

Das SSC/BPO-Umfeld entwickelt sich durch die Digitalisierung stetig weiter. Hierbei sind D-Tools wie RPA, ML und KI inzwischen feste Bestandteile der Prozessoptimierung.

Sie führen dazu, dass die Prozesse wieder ingesourct (weil die Digitalisierung günstiger ist als das bisherige Outsourcing) bzw. gar nicht erst outgesourct werden. Trotzdem bedürfen alle Prozesselemente einer eigenständigen Betrachtung im Rahmen der Sicherheit derartiger effizienzgetriebener Maßnahmen wie Outsourcing und Digitalisierung.

PRÜFUNG VON RPA/ML/KI IM PROZESSUMFELD

Die graduelle Digitalisierung verlangt je nach Level eigenständige Governance- und Risikoanalysen sowie die Implementierung entsprechender Kontrollmaßnahmen bzw. Prüfungshandlungen: Während sich Redesign bis Workflow-Automatisierung normalerweise im SSC/BPO-Umfeld abspielen, bedürfen die erweiterten und kognitiven Digitalisierungsschritte ein besonderes Risk

Assessment. RPA, ML oder KI greifen als externe User auf die Systeme und Prozesse zu und erfordern

- a. eine besondere Governance bei der Entwicklung beispielsweise im Operating Model (OM oder Bot-Fabrik),
- b. eine strenge Absicherung gegen unerlaubten Zugriff und Änderungen des Digitalisierungstools selbst,
- c. ein eigenes Berechtigungskonzept in den Systemen und Prozessen, in denen die D-Tools aktiv Daten be- bzw. verarbeiten,
- d. ein klares Datenkonzept für die von den D-Tools benötigten, verwendeten und bearbeiteten Daten und
- e. ein eigenes IKS für das jeweilige OM sowie eine Integration der operativ aktiven D-Tools in das jeweilige IKS des Unternehmens(prozesses).

Alle Technologien der graduellen Digitalisierung können beispielsweise mittels ISAE 3402 regelmäßig auf Angemessenheit und Effektivität des IKS überprüft werden.

Technologien der graduellen Digitalisierung

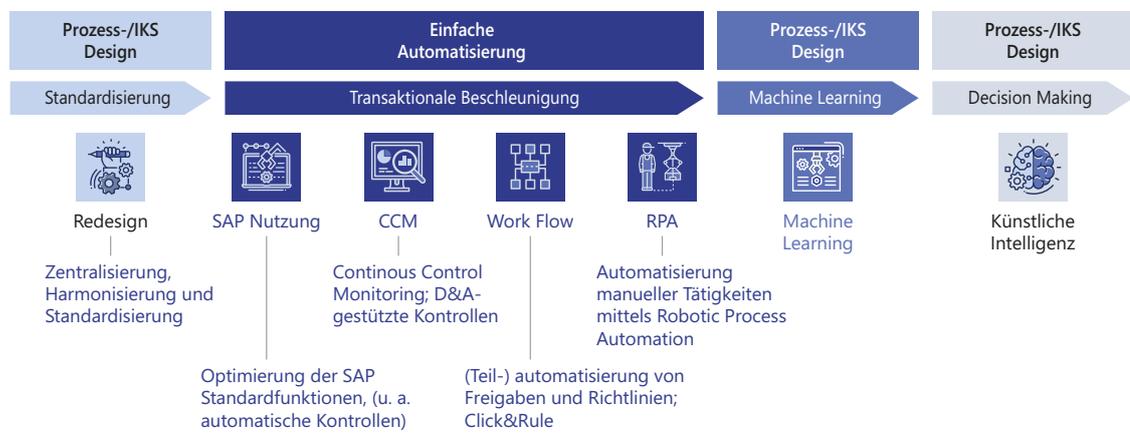


Abbildung 6: Steigender Automatisierungsgrad erhöht die Komplexität der Tools und deren Beherrschung/Überwachung



RPA/ML/KI OPERATING MODEL ALS EIGENER SHARED SERVICE/OUTGESOURCTER PROZESS

Ein professionelles OM wird häufig so ausgestaltet, dass es die entsprechenden Anwendungen für eine größere Gruppe von Einheiten in einem IT-Umfeld entwickelt. Damit stellt es ein SSC eigener Form dar und sollte auch so behandelt werden. Dieses SSC muss über ein eigenes dienstleistungsbezogenes Risikomanagementsystem (RMS) und IKS verfügen, das den genannten Risiken gerecht wird.

Der „Artificial Intelligence in Control“-Ansatz von KPMG umfasst die in Abbildung 7 dargestellten 16 Risk Subjects, die ein angemessenes IKS im RPA/ML/KI-Umfeld abdecken sollte. Diese sind im Rahmen der Analyse zu betrachten, um eine vollständige Risk Map zu erhalten.

Diese Risk Map umfasst mehr als nur den eigentlichen Development-Prozess eines D-Tools. Damit ist aus Sicht des Managements gewährleistet, dass ein Gesamtbild des integrierten RPA/ML/KI OM vorliegt und Kollateralrisiken ausführlich betrachtet werden.

Die 16 Risk Subjects des „Artificial Intelligence In Control“-Ansatzes von KPMG

#	Risk Subjects im RPA-/KI-Umfeld
01	Strategy
02	Governance
03	Human Resource Management
04	Supplier Management
05	Risk Management and Compliance
06	Enterprise Architecture
07	Data and Model Governance
08	Program Governance and Management
09	Solution Development
10	Logging and Monitoring
11	Security Management
12	Identity & Access Management
13	IT Change Management
14	IT Operations
15	Business Continuity
16	Knowledge Management

Abbildung 7: Der umfassende Risikoansatz für eine KI-/RPA-Lösung umfasst 16 Risk Subjects

Um diesen Risiken effektiv gegensteuern zu können, stützt KPMG seinen Prüfansatz auf die Erfüllung der wesentlichen Kriterien, die beim Einsatz von D-Tools als unabdingbar angesehen werden:

Erfüllungskriterien zur effektiven Gegensteuerung der 16 Risk Subjects



Risikoorientierung

Alle Governance-/ IKS-Maßnahmen, auch im Umfeld der D-Tools, müssen sich an den durch die Systeme und Prozesse sowie den Einsatz der Tools entstandenen Risiken orientieren.



Effektivität

Die jeweiligen Kontrollen des IKS sollten immer eine höchstmögliche Effektivität in Bezug auf die abzuwendenden Risiken aufweisen. Dies bedeutet, dass bspw. präventive Kontrollen den detektivischen Kontrollen und automatisierte Kontrollen des gesamten Buchungsstoffes manuellen Stichproben vorzuziehen sind.



Effizienz

Kontrollen müssen gleichzeitig effizient sein, um eine Kostenexplosion der Governance zu vermeiden. Auch hier tragen automatisierte, systemimmanente Kontrollen am meisten zur Effizienzsteigerung bei.

Abbildung 8: Risikoorientierung, Effektivität und Effizienz als wichtige Kriterien zur effektiven Gegensteuerung der 16 Risk Subjects



Bei der Nutzung unternehmensexterner Daten in ML und KI sind folgende Prinzipien zu beachten
**Validierbarkeit**

Die Fähigkeit, den Ursprung von Rohdaten, Trainingsdaten, Modellversuchen und laufenden Änderungen, die vorgenommen werden, jederzeit nachverfolgen zu können.

**Erklärbarkeit**

Die Modelle müssen in der Lage sein, das erlernte Wissen zu erklären und getroffene Entscheidungen in betriebswirtschaftlicher Hinsicht zu erläutern. Zudem werden Interpretationen gewonnen und Erklärungen abgeleitet.

**Fairness**

Die Trainings- / Lerndaten der ML / KI müssen unvoreingenommen sein. Diese und die angewandten Modelle sind hierbei integrativ und vermeiden somit eine ungerechte Behandlung bestimmter Gruppen. Zusätzlich wird die Sicherheit gewährleistet, indem die Modelle einschließlich der Trainer den Richtlinien und Vorschriften entsprechen.

**Interoperabilität**

Die Modelle sind zwischen verschiedenen Laufzeiten, Anbietern oder Frameworks kompatibel. Zugleich sind die Modelle, die Genauigkeit der Klassifizierung des Trainingsatzes (Ground Truth) und das Feedback geschützt vor Schäden oder feindlichen Angriffen.

 Abbildung 9: Die vier Prinzipien der Nutzung unternehmensexterner Daten in ML und KI

Bei der Risikoanalyse der von ML oder KI verwendeten Daten sollten insbesondere folgende Gesichtspunkte berücksichtigt werden:

- Eigenschaften, die für das Verständnis der Daten und Datenbezüge erforderlich sind. Diese sind bspw. Datenvolumen, Format der Eingangsvariablen, Korrelations und Co-Varianzen-Analyse und fehlende Input-Variablen.
- der Datenaufbereitungsprozess zur Verarbeitung der Daten in den ML/KI-Modellen, unter anderem ein abgesicherter Datentransformationsprozess
- Überprüfung der Datenqualität aller für das Trainieren des Modells verwendeten Third Party Data.

Darüber hinaus sind weitere Kontrollen im ML / KI Prozess zu berücksichtigen, die eine angemessene Überprüfung des Verarbeitungsprozesses und Output-Reviews sicherstellen sowie eine periodische Überprüfung der Algorithmen und ihrer Ergebnisse auf Konsistenz und Korrektheit ermöglichen.

SICHERHEIT ÜBER DIVERSE TECHNOLOGIE- UND ORGANISATIONS-LEVELS VON SSC/BPO UND D-TOOLS

Die Sicherheit der diversen RPA/ML/KI OM kann wie die SSC-Prozesse selbst am besten mittels einer gesonderten IKS-Prüfung abgedeckt werden. Dazu dient beispielsweise der ISAE 3402 als Standard für Prüfungen der dienstleistungsbezogenen internen Kontrollsysteme, die ein Wirtschaftsprüfer durchführen kann.

Die drei wesentlichen Ebenen des Operating Models für Digital Tools

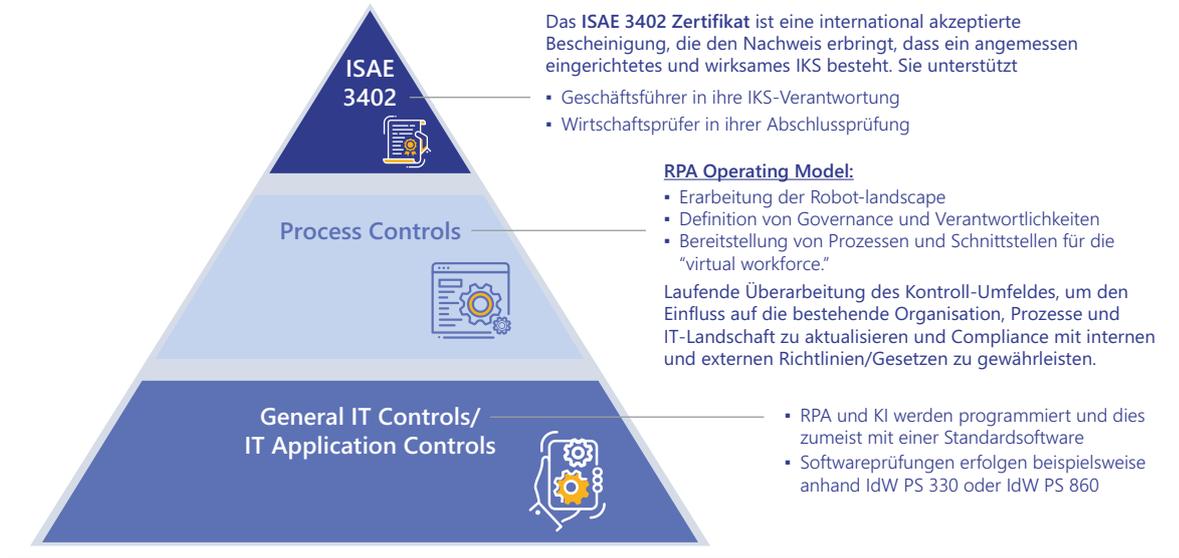


Abbildung 10: Sicherheit durch die Prüfung der KI-Fabrik/des RPA Operating Model

Die Prüfung des D-Tool OM erfolgt auf drei wesentlichen Ebenen, deren Komplexität aber durch die nachfolgend beschriebene Modularisierung beliebig gesteigert werden kann:

- Die IT-Systemprüfung der genutzten Software-Applikation einschließlich der dazu gehörenden Betriebssysteme und Hardware (GITC-Prüfung)
- Prüfung der OM-immanenten Prozesskontrollen
- Prüfung aller weiteren IKS-relevanten Kontrollen aus dem Kontrollumfeld, den Informationsflüssen und dem Risikomanagementsystem (s. o.).

Hierbei ist es durchaus hilfreich, das OM von Anfang an in das IKS des Konzerns (soweit es ein „captive“ SSC-Modell ist) zu integrieren und damit beispielsweise dem COSO-Framework (The Committee of Sponsoring Organizations of the Treadway Commission) zu unterwerfen, das die meisten Großkonzerne zumindest im Ansatz ihrem eigenen IKS zugrunde legen.

Weitere zu beachtende Komplexitäten sind die bereits erwähnte Modularisierung und Fragmentierung ausge-

lagerter Prozesse, wobei diese Module oftmals weiter outgesourct werden und das Outsourcing wiederum über mehrere Ebenen erfolgen kann.

Diese Form der mehrstufigen Auslagerung kann dazu führen, dass das auslagernde Unternehmen den Überblick über die verschiedenen Ebenen der Auslagerung verliert: Ein Kunde („user entity“) übergibt den Prozess an einen BPO-Provider, dieser sourct Teile an einen Sub-Unternehmer aus und dieser wieder an einen Cloud-Provider, der wiederum eine Server-Farm beauftragt; am Ende weiß der Kunde nicht mehr, wer alles an seinem Prozess beteiligt ist.

Die heutigen SLAs sollten diese Tatsache berücksichtigen und eine entsprechende Verpflichtung der SSC/BPO-Provider vornehmen. Inhalt der Verpflichtung sollte es sein, die im Outsourcing-SLA vereinbarten Bedingungen auf den weiteren Ebenen ebenfalls aufzunehmen. Grundsätzlich werden die SSC/BPO verpflichtet, nicht nur für ihr eigenes, sondern auch für alle Sub-Unternehmer und deren Sub-Unternehmer die gleiche Compliance wie für das outsourcende Unternehmen sicherzustellen und zu überwachen. Während das



Sicherstellen zumeist vertraglich abgesichert wird, mangelt es in der Regel an der Überwachung.

Die vertragliche Vereinbarung entbindet das Management des auslagernden Unternehmens nicht von seiner Haftung für den Gesamtprozess und seiner Verpflichtung, angemessene Maßnahmen zu implementieren, um diese Kette zu überwachen. In den allermeisten Fällen wird der ISAE-3402-Bericht des SSC/BPO nach der Carve-out-Methode erstellt, sodass die IKS der Sub- und Sub-Sub-Unternehmer nicht mit abgedeckt sind. Hier gilt es, zwei Kontrollmaßnahmen zu implementieren:

1. Der SSC/BPO-Provider selbst muss Kontrollen implementiert haben, die die Prozessaktivitäten der Sub- und Sub-Sub-Unternehmer absichern. Hier fehlt es aus Sicht von KPMG noch in den meisten Fällen daran, dass in vielen ISAE-3402-Berichten nicht angemessen über die Auslagerung und die entsprechenden Sub- und Sub-Sub-Unternehmer berichtet wird. Das auslagernde Unternehmen kann dies so nicht akzeptieren.
2. Soweit die Sub-Unternehmen über eigene IKS verfügen und diese auch geprüft wurden, sollte der SSC/BPO-Provider diese Prüfberichte erhalten und soweit gewünscht auch an das auslagernde Unternehmen weiterleiten.

Der Abschlussprüfer selbst wird sich die Finanzprozesse und alle weiteren relevanten finanznahen Prozesse ansehen und prüfen. Soweit er das Management, den PA bzw. den AR hierüber in Kenntnis setzt, kann sich der PA/AR ein besseres Bild von den Prozessen verschaffen und dies seiner eigenen IKS-Beurteilung zugrunde legen. Allerdings verlangt der § 107 (3) AktG vom Kontrollgremium, dass es sich eigenständig einen Überblick über die Wirksamkeit des gesamten RMS und IKS (sowie der Internen Revision) des Unternehmens verschaffen muss. Dies bedeutet aus Governance-Perspektive, dass

- a. der PA/AR zusammen mit dem Vorstand/der Geschäftsführung eine Übersicht aller RMS- bzw. IKS-relevanten Prozesse erstellen muss,

- b. jemanden beauftragen muss, in seinem Namen die dazu vorhandenen RMS und IKS zu beurteilen und an den PA/AR zu berichten,
- c. es nicht ausreicht, den Bericht entgegenzunehmen; der PA/AR muss sich anhand weiterer Unterlagen, Informationen, Berichte und Präsentationen von der Plausibilität der IKS-Beurteilung überzeugen.

In einem nach US-Vorschriften gelisteten Unternehmen wird dieser Prozess seit 2003 bereits im Sarbanes-Oxley Act (SOX 404) begründet. So wird neben der eigentlichen Tätigkeit des Prüfers zusätzlich ein eigenständiges Management-Assessment verlangt. Der AR/PA kann durchaus einen Wirtschaftsprüfer als Subdienstleister beauftragen, allerdings darf dies weder der Abschlussprüfer sein noch können Management, PA bzw. AR sich ihrer Eigenverantwortung entziehen.

WIE WEIT SIND DIE STANDARD-SETTER (IDW, ISAAC, FASB ...) BEI DIESER THEMATIK?

Es ist für Abschlussprüfer und Unternehmen bei steigender Nutzung der D-Tools durchaus interessant zu verstehen, wo die Standard-Setter bei der Erstellung von Prüfungsstandards zum Thema „Prüfung von RPA/ML/KI“ sind. Der US-amerikanische Verband der Wirtschaftsprüfer (AICPA) hat seine Standards dahin gehend angepasst, dass er auf der Basis des COSO Framework eine angemessene Prüfung des IKS über die OM der D-Tools gewährleistet. Allerdings sind diese Regularien bis dato noch nicht in einem eigenen Standard dokumentiert worden, sondern beruhen auf bestehenden Standards, die insbesondere auf die Prüfung der General IT Controls (GITC) aufbauen und diese um notwendige Schritte zur Abdeckung der Besonderheiten des jeweiligen D-Tools erweitern.

KPMG arbeitet derzeit an einem eigenen Prüfungsstandard, um diesen als Diskussionsgrundlage in nationalen wie auch internationalen Gremien einzubringen. Damit bekämen Prüfer und geprüfte Unternehmen mehr Verlässlichkeit im Prüfungsprozess für Sicherheit in Outsourcing und Digitalisierung.



Fazit und Zusammenfassung



Digitalisierung mittels RPA/ML/KI (D-Tools) wird inzwischen vielfältig genutzt, um Prozesse weiter zu optimieren und Kosten einzusparen. Dabei ersetzen D-Tools teilweise bisher im SSC gebündelte oder outgesourcte Prozessmodule.



Sowohl die D-Tools als auch andere kostengetriebene Maßnahmen führen zu einer weiteren Zersplitterung von Prozessen. Die dabei entstehenden Einzelmodule werden wiederum oftmals über mehrere Sub-Unternehmen ausgelagert.



D-Tools bringen – wie jede neue Technologie – neue Risiken und Kontrollen mit sich, die entsprechend zu erfassen und zu behandeln sind (RMS).



Das Management des auslagernden Unternehmens inkl. Prüfungsausschuss (PA) und Aufsichtsrat (AR) bleibt weiterhin in vollem Umfang für die ausgelagerten und neuen Prozesselemente verantwortlich. Der PA/AR ist verpflichtet, sich regelmäßig über die Wirksamkeit von RMS und IKS zu überzeugen.



Vor diesem Hintergrund ist es notwendig, dass der (Abschluss-)Prüfer zusammen mit dem auslagernden Unternehmen das jeweilige RPA/ML/KI Operating Model anhand geeigneter Ansätze, z. B. der Risk Subjects, analysiert und eine angemessene IKS-Implementierung prüferisch begleitet.



Wesentliche Kriterien zur optimalen Ausgestaltung des IKS sind die vorrangige Risikoorientierung, die Effektivität der Kontrollen und die Effizienz der Kontrolldurchführung, damit die notwendige Governance nicht zulasten der Kosten geht.



Eine Standardisierung des Prüfungsansatzes zur Digitalisierung und den D-Tools wird beiden Parteien, Mandant wie Abschlussprüfer, zusätzliche Sicherheit geben und sollte daher auch zeitnah erarbeitet werden. KPMG wird seinen Anteil dazu als Standard-Setter erbringen, damit die Sicherheit in Outsourcing und Digitalisierung auch zukünftig für Management, PA und AR wie auch für die Abschlussprüfung gegeben ist.

Die Digitalisierung und Automatisierung schreitet auch in den Finanz- und anderen Unterstützungsprozessen der Unternehmen voran. Dabei ersetzen D(igitalisierungs)-Tools wie RPA, ML und KI auch bisher outgesourcte Prozessschritte und -module und gestalten diese effizienter. Die voranschreitende Modularisierung führt zu einer immer komplexeren Prozessstruktur mit vielen nachgeschalteten Akteuren – insbesondere im SSC/ BPO-Umfeld.

Daher ist es notwendig, dass hier auch die Governance Schritt hält und bei der Ausgestaltung der Prozesse, der Entwicklung von D-Tools wie auch beim Out- und Insourcing das Risikomanagement aktualisiert und dass das IKS an die neuen Risiken angepasst wird. Die regelmäßige Überprüfung dieser Bereiche sollte zum Standardrepertoire der internen und externen Überwachungsmaßnahmen gehören.

KPMG arbeitet daran, dass für diese Prüfung angemessene Standards entwickelt werden.

UNTERNEHMENSPORTRÄT



KPMG

KPMG ist ein weltweites Netzwerk mit rund 207.000 Mitarbeitern in 152 Ländern und Territorien. Auch in Deutschland gehört KPMG zu den führenden Wirtschaftsprüfungs- und Beratungsunternehmen und ist mit rund 11.300 Mitarbeitern an 25 Standorten präsent. Unsere Leistungen sind in die Geschäftsbereiche Audit, Tax, Consulting und Deal Advisory gegliedert.

KPMG betreut Mandanten jeder Größe und aus allen Branchen – vom mittelständischen Autozulieferer über die Regionalbank bis hin zu internationalen Pharma- oder Medienunternehmen. Für wesentliche Branchen unserer Wirtschaft haben wir eine geschäftsbereichsübergreifende Spezialisierung vorgenommen. Hier laufen die Erfahrungen unserer Experten weltweit zusammen und tragen zusätzlich zur Beratungsqualität bei.

Shared Services & Outsourcing Assurance

Im Geschäftsbereich Audit/Corporate Governance Services bietet KPMG mit den „Shared Services & Outsourcing Assurance“ Prüfungs- und Beratungsdienstleistungen rund um das Thema Shared Services und Outsourcing.

Dazu gehören Assurance-Dienstleistungen im Rahmen des Outsourcings (ob an ein „captive“ SSC oder einen BPO-Provider) genauso wie Optimierungsberatung bei bestehenden SSC und BPO sowie im Übergang zu D-Tool-Anwendungen. Weitere Dienstleistungen umfassen u. a. Unterstützungsleistungen hinsichtlich der Entwicklung bzw. der Prüfung von RPA-Lösungen.

Die Prüfungen im SSC-Umfeld werden im Wesentlichen anhand der Standards ISAE 3402 oder PS 951 n. F. durchgeführt; dabei können auch die Besonderheiten wie die SOC-II-Vorschriften und oder beispielsweise BSI/C5-Regeln bei Cloud-Providern angewandt werden.

KONTAKT

KPMG AG Wirtschaftsprüfungsgesellschaft
Thomas Kern, Wirtschaftsprüfer, Steuerberater
Partner Shared Services & Outsourcing Assurance
Head of SSC-Audit and ISAE 3402 – Accreditation
Schlossgartenstraße 1, 68161 Mannheim
Telefon: +49 (0) 6 21 42 67 - 502
E-Mail: tkern1@kpmg.com
Internet: www.kpmg.de

KONTAKT

KPMG AG Wirtschaftsprüfungsgesellschaft
Roxana Meschke
Partner Audit
Compliance Governance Services
The Squire, 60549 Frankfurt am Main
Telefon: +49 (0) 69 95 87 - 3428
E-Mail: rmeschke@kpmg.com
Internet: www.kpmg.de



Lünendonk & Hossenfelder

Die Lünendonk & Hossenfelder GmbH (Mindelheim) untersucht und berät europaweit Unternehmen aus der Informationstechnik-, Beratungs- und Dienstleistungs-Branche. Mit dem Konzept Kompetenz³ bietet Lünendonk & Hossenfelder unabhängige Marktforschung, Marktanalyse und Marktberatung aus einer Hand. Der Geschäftsbereich Marktanalysen betreut seit 1983 die als Marktbarometer geltenden Lünendonk®-Listen und -Studien sowie das gesamte Marktbeobachtungsprogramm.

Die Lünendonk®-Studien gehören als Teil des Leistungsportfolios der Lünendonk & Hossenfelder GmbH zum „Strategic Data Research“ (SDR). In Verbindung mit den Leistungen in den Portfolio-Elementen „Strategic Roadmap Requirements“ (SRR) und „Strategic Transformation Services“ (STS) ist Lünendonk & Hossenfelder in der Lage, ihre Beratungskunden von der Entwicklung der strategischen Fragen über die Gewinnung und Analyse der erforderlichen Informationen bis hin zur Aktivierung der Ergebnisse im operativen Tagesgeschäft zu unterstützen.

KONTAKT

Lünendonk & Hossenfelder GmbH
Jonas Lünendonk
Maximilianstraße 40, 87719 Mindelheim
Telefon: +49 (0) 82 61 7 31 40 - 13
Telefax: +49 (0) 82 61 7 31 40 - 66
E-Mail: j.luenendonk@luenendonk.de
Internet: www.luenendonk.de

BILDERQUELLEN

Titel	© AdobeStock / denisismagilov
	© AdobeStock / pixeltrap
	© AdobeStock / fgnopporn
	© AdobeStock / Jakub Jirsák
	© AdobeStock / WrightStudio
Inhalt	© AdobeStock / WrightStudio
Seite 4	© AdobeStock / WrightStudio
Seite 6	© AdobeStock / Jakub Jirsák
Seite 8	© AdobeStock / phonlamaiphoto
Seite 10	© AdobeStock / Egor
Seite 12	© AdobeStock / Murrstock



ÜBER LÜNENDONK & HOSSFELDER

Seit 1983 ist die Lünendonk & Hossenfelder GmbH spezialisiert auf systematische Marktforschung, Branchen- und Unternehmensanalysen sowie Marktberatung für Informationstechnik-, Beratungs- und weitere hochqualifizierte Dienstleistungsunternehmen. Der Geschäftsbereich Marktforschung betreut die seit Jahrzehnten als Marktbarometer geltenden Lünendonk®-Listen und -Studien sowie das gesamte Marktbeobachtungsprogramm. Die Lünendonk®-Studien gehören als Teil des Leistungsportfolios der Lünendonk & Hossenfelder GmbH zum „Strategic Data Research“ (SDR). In Verbindung mit den Leistungen in den Portfolio-Elementen „Strategic Roadmap Requirements“ (SRR) und „Strategic Transformation Services“ (STS) ist Lünendonk & Hossenfelder in der Lage, ihre Kunden von der Entwicklung strategischer Fragen über die Gewinnung und Analyse der erforderlichen Informationen bis hin zur Aktivierung der Ergebnisse im operativen Tagesgeschäft zu unterstützen.

Managementberatung

Informations- und
Kommunikations-Technik

Wirtschaftsprüfung /
Steuerberatung

Technologie-Beratung /
Engineering Services

Zeitarbeit /
Personaldienstleistungen

Facility Management /
Industrieservice



IMPRESSUM

Herausgeber:

Lünendonk & Hossenfelder GmbH
Maximilianstraße 40
87719 Mindelheim

Telefon: +49 (0) 82 61 7 31 40 - 0

Telefax: +49 (0) 82 61 7 31 40 - 66

E-Mail: info@lunenendonk.de

Internet: www.lunenendonk.de

Erfahren Sie mehr unter

www.lunenendonk.de

Autor:

Jonas Lünendonk, Lünendonk & Hossenfelder GmbH

Gestaltung:

K16 GmbH, Hamburg

Copyright © 2019 Lünendonk & Hossenfelder GmbH, Mindelheim

Alle Rechte vorbehalten

