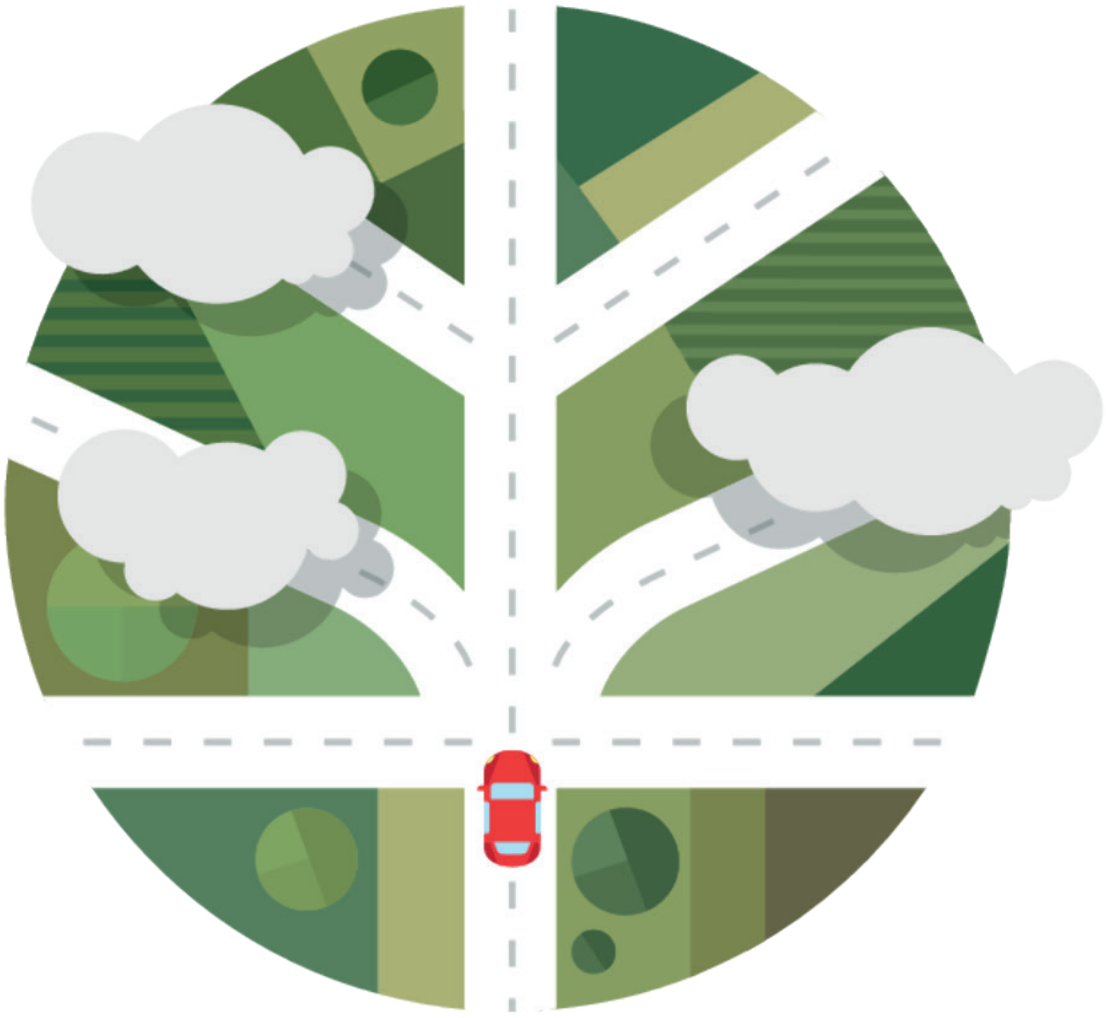
Deloitte.



Fahrplan Automatisierungsgrad

Wie Banken die Kontrolle über die IT-Schattenwirtschaft zurückgewinnen

Excel wird zum Problem

Das Risikoreporting ist in vielen Banken von manuellen Datenverarbeitungslösungen geprägt. Diese Umgehungslösungen sollen zukünftig stärker reguliert und eingedämmt werden.

Vor dem Hintergrund zunehmender und immer kurzfristigerer Ad-hoc-Berichtsanforderungen und Bankenstresstests durch nationale und internationale Aufsichtsbehörden sind flexible Datenverarbeitungslösungen für Banken unverzichtbar. Da oftmals zeitnah Veränderungen von Rahmenbedingungen, Parametern, Berichtsinhalten und -formaten berücksichtigt werden müssen, kommen in vielen Instituten individuelle Datenverarbeitungslösungen (IDV) zum Einsatz. Häufig werden entlang der gesamten Verarbeitungskette Anreicherungen, Berechnungen, Abgleiche oder Datenaufbereitungsschritte in flexible Spreadsheets und benutzerindividuelle Datenbanken ausgelagert. Der Einsatz von IDV bietet vor allem eine schnell verfügbare, kostengünstige und benutzerindividuelle Alternative zu aufwendigen EDV-Einführungen. IDV-Lösungen, die in der Regel nur als Übergangslösung entwickelt wurden, mutieren in der Folge nicht selten zu EDV-Ersatzprodukten, die schwer zu durchschauen und noch schwerer wieder abzulösen sind. In ansonsten automatisierten Prozessketten integriert, erhöht der Einsatz von IDV das Risiko unzulässiger Eingriffe und der Entstehung von Verarbeitungsfehlern, die sich einer systematischen Datenqualitätssicherung und Kontrolle entziehen.

Wärend die Beaufsichtigungspraxis der vergangenen Jahre mit zum Aufbau der IT-Schattenwirtschaft beigetragen hat, sind IDV-Lösungen nun selbst ins Fadenkreuz der Bankenaufsicht gerückt.
Im Zuge der zunehmenden Regulierung von Datenverarbeitungs- und Berichtsprozessen gerät auch der Einsatz von IDV in den Fokus der Bankenaufsicht. Diese verfolgt das Ziel, den Automatisierungsgrad der Banken – also das Verhältnis von durch die IT betreuten Applikationen zu individuellen Datenverarbeitungslösungen der Endbenutzer – zu steigern. Eine intransparente und schwer kontrollierbare IT-Schattenwelt wird aufgrund des hohen Fehlerrisikos nicht mehr als Grundlage von Berichts- und Steuerungsprozessen akzeptiert.

In Deutschland sind durch die Grundsätze für die effektive Aggregation von Risikodaten und die Risikoberichterstattung (BCBS #239) [1] und deren Integration in die Mindestanforderungen an das Risikomanagement (MaRisk) [2] alle Banken angesprochen.

„Vielen Kunden wird das Ausmaß der selbst gebauten Excel- und Access-Lösungen erst in regulatorischen Umsetzungsprojekten wirklich bewusst."
Stefanie Kampmann
Partnerin bei Deloitte

[1] BCBS #239 (Grundsatz 3, Tz. 38): „Zwischen automatisierten und manuellen Systemen sollte ein angemessenes Gleichgewicht bestehen. Ist ein fachliches Urteil erforderlich, dürften menschliche Eingriffe angebracht sein. Hingegen ist bei zahlreichen anderen Prozessen ein höherer Grad an Automatisierung wünschenswert, um die Fehlerwahrscheinlichkeit so gering wie möglich zu halten."

[2] MaRisk (AT 4.3.4, Tz.3): „Der Einsatz und der Umfang manueller Prozesse und Eingriffe sind zu begründen und zu dokumentieren und auf das notwendige Maß zu beschränken." **Sowie MaRisk (AT 7.2, Tz. 5):** „Die Anforderungen aus AT 7.2 (Hinweis Deloitte: Anforderungen an IT-Systeme) sind auch beim Einsatz von durch die Fachbereiche selbst entwickelten Anwendungen (Individuelle Datenverarbeitung – „IDV") entsprechend der Kritikalität der unterstützten Geschäftsprozesse und der Bedeutung der Anwendungen für diese Prozesse zu beachten."

Das konkrete Anspruchsniveau an den erwarteten Automatisierungsgrad und die Bewertung der Angemessenheit und Ausgestaltung von IDV wurden durch die Autoren der BCBS #239-Grundsätze und der MaRisk offengehalten und sind im Einzelfall durch die Aufseher zu bewerten. Insofern besteht bei den Instituten Unsicherheit bezüglich der Zielsetzung und der richtigen Priorisierung für die Ablösung bzw. Absicherung der hauseigenen IT-Schattenwelt.

Angesichts der engen Fristen für die Umsetzung von BCBS #239 und den neuen MaRisk-Bestimmungen müssen betroffene Banken einen klaren Fahrplan zur Herstellung eines angemessenen Automatisierungsgrades verfolgen und sollten im Fall von Prüfungen durch die Aufsicht auf konkrete Maßnahmen verweisen können.

Die Probleme beginnen meist schon bei der Definition von IDV und bei der Frage, welche Bewertungsmaßstäbe anzuwenden sind.

In den meisten Instituten wird der Einsatz von IDV zwar formal geregelt, häufig aber ohne die notwendige Konsequenz und Durchschlagskraft. Die Probleme beginnen meist schon bei der Definition von IDV und der Frage, welche Bewertungsmaßstäbe bei der Risikoeinstufung anzuwenden sind: Nicht jedes Excel-Spreadsheet oder jede benutzerindividuelle Datenbank muss zwingend als IDV klassifiziert werden oder ein signifikantes Fehlerrisiko darstellen.

Daher ist eine Einzelfallprüfung nach klar definierten Kriterien unumgänglich, um Kritikalität und Fehlerrisiken einer IDV-Anwendung für die zugrundeliegenden Prozesse zu bewerten. Ausgehend von dieser Risikoeinstufung ist zu entscheiden, wie die IDV-Anwendung zu behandeln ist.

Auch wenn Aufseher eine weitgehende IDV-Ablösung fordern, ist Augenmaß geboten. Eine kurzfristige Ablösung ist nicht immer zielführend. So sind Mindeststandards für Test- und Kontrollverfahren zu definieren, mit denen verbleibende IDV-Lösungen, ggf. abgestuft nach ihrer Kritikalität, abzusichern sind. Auf längere Sicht müssen betroffene Institute ihren Anspruch zur Reduzierung manueller Eingriffe in kritische Datenverarbeitungsprozesse mit entsprechenden Maßnahmen untermauern.

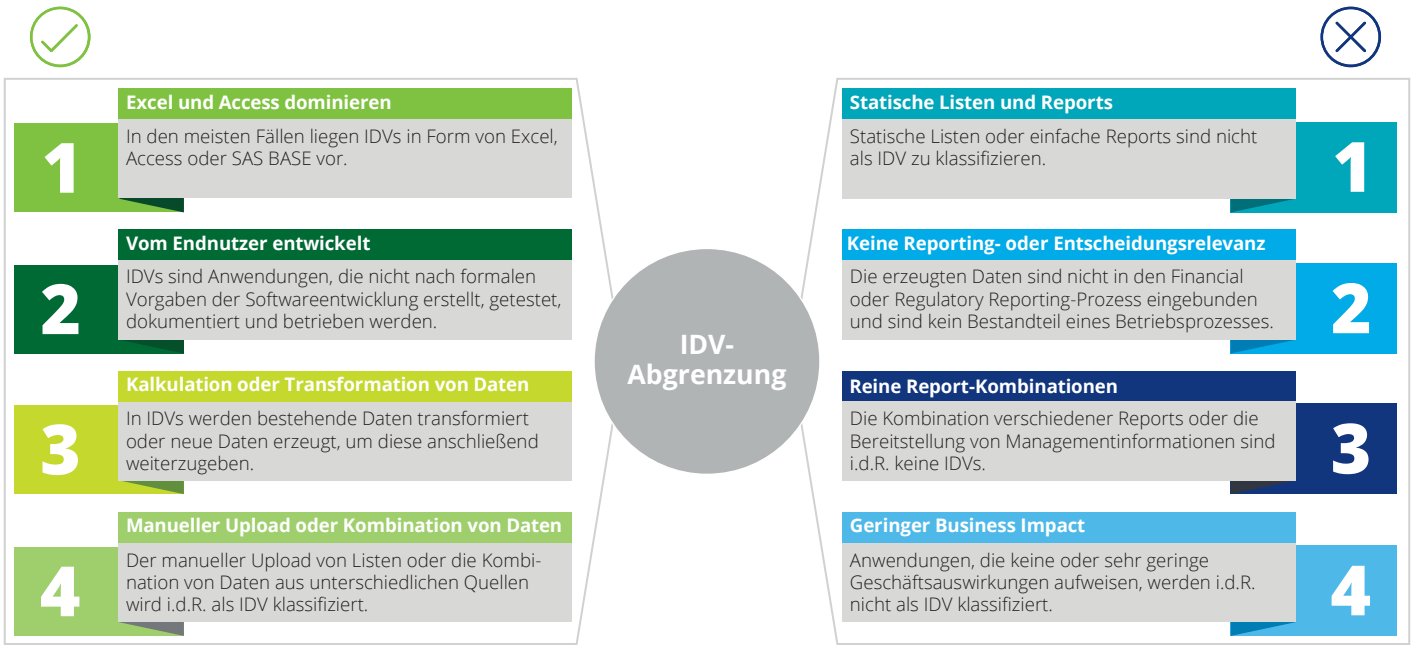
Automatisierungsgrad beurteilen und steuern

Deloitte hat ein praxisnahes Vorgehensmodell zur Beurteilung von IDV-Lösungen entwickelt, bei dem solche Anwendungen mithilfe eines umfassenden Bewertungskataloges systematisch durchleuchtet und vorhandene Kontrollen erhoben werden. Das Ergebnis ist eine nachvollziehbare Dokumentation des Risikoprofils sowie vorhandener Kontrolllücken in Bezug auf einzelne IDV-Anwendungen. Können oder sollen diese nicht kurzfristig abgelöst werden, leiten sich aus der Analyse notwendige Maßnahmen für die Absicherung ab. So kann ein angemessener Automatisierungsgrad gegenüber der Aufsicht begründet und im Zusammenhang mit geplanten Maßnahmen zur Automatisierung oder Absicherung schlüssig untermauert werden (s. Abb. 1).

01// Klassifizierung IDV-unterstützter Prozesse

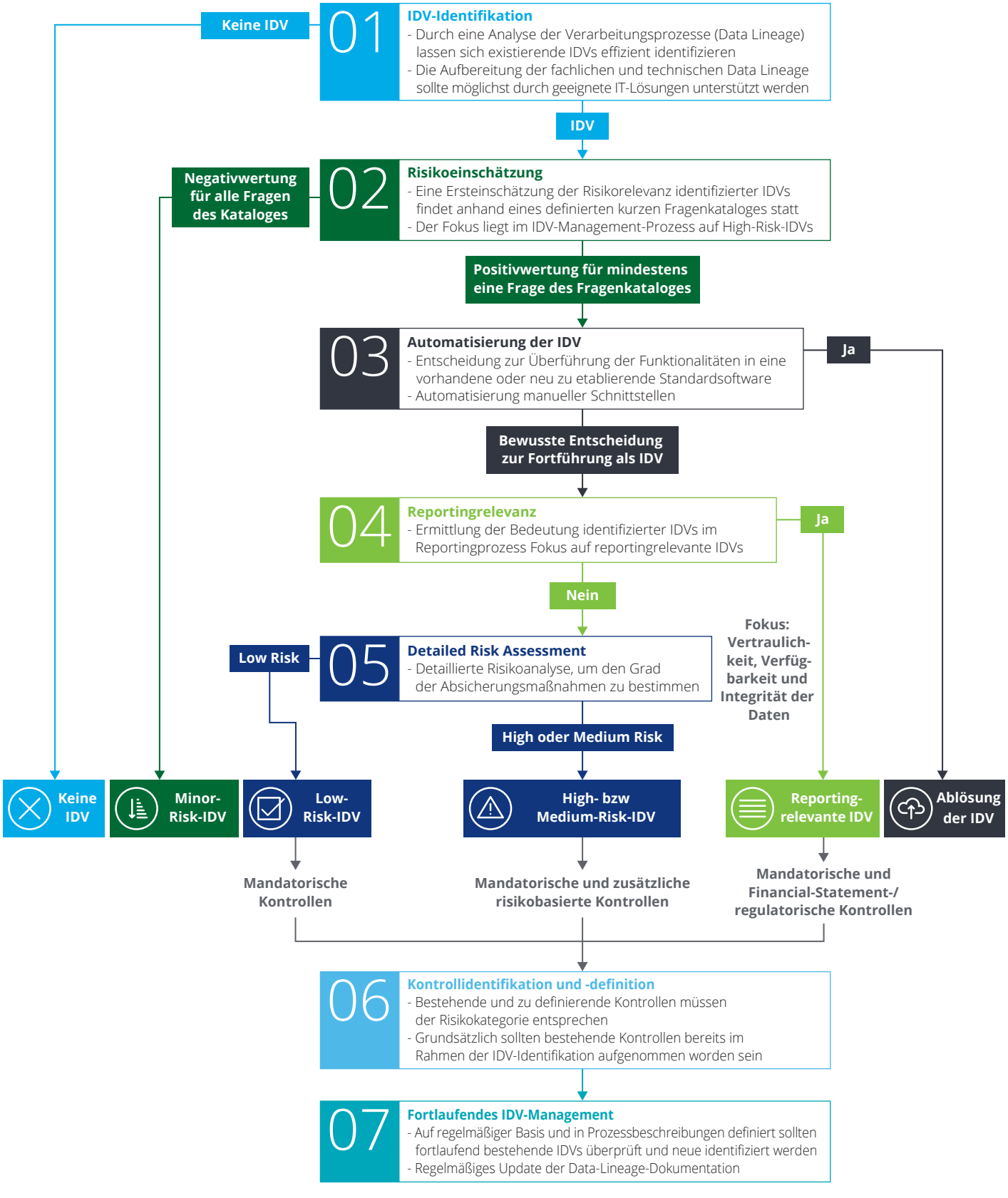
Grundlage für die Beurteilung und Steuerung eines angemessenen Automatisierungsgrades ist die systematische Aufnahme und Dokumentation von Datenverarbeitungsprozessen.[1] Transparenz über den Gesamtverarbeitungsprozess (front-to-end) ist Voraussetzung für die strukturierte Erhebung und Klassifikation der manuellen Prozesseingriffe und IDV-Anwendungen. Die IDV-Klassifizierung erfolgt kriterienbasiert, unter Berücksichtigung von Art, Beschaffenheit und Verwendungszweck der Lösung. In diesem Schritt werden nicht IDV-relevante Sachverhalte für die weitere Analyse ausgesteuert (s. Abb. 2).

Abb. 1 – Deloitte Vorgehensmodell



[1] Deloitte schlägt ein geeignetes Vorgehen zur Prozessdokumentation in einem separaten Papier „BCBS #239-konforme Prozessdokumentation" vor.

Abb. 2 – Kriterien zur Abgrenzung von IDV



02// Ersteinschätzung Risikorelevanz

Die als IDV klassifizierten Anwendungen werden einer Ersteinschätzung unterzogen, bei der diejenigen gekennzeichnet werden, von denen kein Risiko für geschäftskritische Prozesse und IT-Systeme ausgeht. Für die weiteren Schritte sind diese IDV-Anwendungen nicht relevant.

03// Ablösungsstrategien

Für alle verbleibenden IDV-Anwendungen wird das Automatisierungspotenzial untersucht. Für solche Anwendungen, die nicht abgelöst werden können bzw. sollen, wird eine Begründung für den dauerhaften Einsatz dokumentiert. Alle Übrigen werden mit konkreten Maßnahmen und dem geplanten Zeitpunkt der Ablösung unterlegt. IDVs, die kurzfristig abgelöst werden können, werden von der weiteren Risikoanalyse ausgeschlossen.

04// Steuerungs- und Berichtsrelevanz

Das Hauptaugenmerk der Analyse liegt auf dem Einsatz von IDVs zur Erzeugung und Verarbeitung von steuerungs- und berichtsrelevanten Daten. Betroffene IDVs werden der höchsten Risikostufe zugeordnet und unterliegen bis zu ihrer Ablösung strengen Absicherungsstandards.

05// Weitere Risikoabstufung

Für nicht unmittelbar steuerungs- oder reportingrelevante IDV-Anwendungen erfolgt eine Risikoabstufung unter Berücksichtigung der Vertraulichkeit, Integrität und Verfügbarkeit der enthaltenen Daten. Dabei werden finanzielle Risiken, aber auch Reputations-, Markt- und regulatorische Risiken bewertet.

06// Absicherungsstrategien

Auf Grundlage der vorangegangenen Risikobewertung wird das zukünftige Kontrollumfeld definiert, das zur temporären oder dauerhaften Absicherung kritischer IDV-Lösungen benötigt wird. Dazu werden zunächst vorhandene Kontrollen erfasst. Das Kontrollniveau im Status quo wird mithilfe eines Fragenkataloges erhoben und offenbart eventuelle Kontrolllücken in Abhängigkeit von der Risikostufe der einzelnen IDV. Während bei Lösungen mit einer geringen Risikoeinstufung lediglich mandatorische Kontrollen notwendig erscheinen, die vor unberechtigten Zugriffen oder Änderungen der IDV schützen sollen, sind bei allen anderen Klassifikationen die Kontrollen in Abhängigkeit vom mit der IDV verbundenen Risiko auszuprägen.

07// Steuerung Automatisierungsgrad

Im Rahmen des dargestellten Vorgehensmodells werden umfassende Erkenntnisse zur Kritikalität von temporären und dauerhaften IDV-Anwendungen gesammelt und an zentraler Stelle übersichtlich dokumentiert. Aus diesen Erkenntnissen leiten sich Notwendigkeit und Priorität von Maßnahmen im Einzelfall nachvollziehbar ab. Ein vorgefertigtes Template liefert alle relevanten Fragen für die Risikoeinstufung und ermöglicht eine effiziente Erhebung der IDV-Lösungen und des Kontrollumfelds.

Absicherung von IDV mit Augenmaß

Der Einsatz von IDV wird aufgrund der Zeit- und Kostenvorteile gegenüber klassischen IT-Systemen und aufgrund der höheren Flexibilität auch in Zukunft zur Praxis der Datenverarbeitung in Banken gehören. Durch die strengere Regulierung werden jedoch vermeintliche Vorteile individueller Lösungen deutlich beschnitten. Insbesondere die von Aufsehern erwarteten Absicherungen durch angemessene Test- und Kontrollverfahren erhöhen den Aufwand im Umgang mit IDV signifikant.

Für permanente IDV-Lösungen lohnt es sich daher, über neue Wege nachzudenken. Deloitte bietet mit dem innosys-Framework die Möglichkeit der Vollintegration diverser IDV-Lösungen in einen geordneten IT-Betrieb. innosys basiert auf MS SQL Server und Longview Analytics und lässt sich als flexibles Toolset einfach auf die individuelle Systemarchitektur des Institutes zuschneiden. Für schützenswerte IDV-Anwendungen ermöglicht innosys eine nahtlose Integration in einen abgesicherten und revisionssicheren IT-Betrieb. Darüber hinaus bietet das modulare Framework die Möglichkeit zur selbstständigen Weiterentwicklung und Ausweitung für institutsspezifische Zwecke. In vielen Fällen stellt innosys eine kostengünstige, intuitive, schnell verfügbare und trotzdem nachhaltige Alternative zur Ablösung von IDV-Anwendungen dar.

Mit innosys gelingt ein angemessener Automatisierungsgrad
Der erste Schritt zur Ablösung von IDVs ist klar: Die bestehenden Anwendungen müssen identifiziert, katalogisiert und bewertet werden. Einige lassen sich anschließend unkompliziert durch eine EDV-Überführung beseitigen. Andere erweisen sich als unverzichtbar, müssen jedoch angemessen abgesichert werden. Für diesen Zweck haben Deloitte-Experten innosys entwickelt. Als unkomplizierte, revisionssichere und universelle Lösung lassen sich mit innosys die Vorteile von IDV mit regulatorischen Anforderungen vereinbaren. So lässt sich nicht nur die bestehende IDV in Einklang mit aufsichtsrechtlichen Vorgaben absichern und automatisieren. Auch für zukünftige Anwendungsfälle bietet sich mit innosys eine flexible und sichere Lösung für den Umgang mit zukünftigen IDV-Entwicklungen.

Deloitte unterstützt Sie gerne mit individuell abgestimmten Lösungsansätzen und Konzepten auf Ihrem Weg zu einem angemessenen Automatisierungsgrad.

Ihre Ansprechpartner

Stefanie Kampmann
Partner
Financial Services Solutions
Tel: +49 (0)69 9713 7517
stkampmann@deloitte.de

Tobias Piegeler
Director
Financial Services Solutions
Tel: +49 (0)211 8772 4154
tpiegeler@deloitte.de

Simon Sulzbach
Senior Manager
Financial Services Solutions
Tel: +49 (0)69 9713 7424
ssulzbach@deloitte.de

Maximilian Ormian
Manager
Financial Services Solutions
Tel: +49 (0)69 9713 7293
mormian@deloitte.de

Bengt Ebeling
Senior Consultant
Financial Services Solutions
Tel: +49 (0)40 32080 4462
bebeling@deloitte.de

Deloitte.

Stand 5/2018