Lukas Görnert
Dezember/2019

DER UMGANG MIT SCHATTEN-IT IM BANKENSEKTOR – IDV-ANWENDUNGEN IM KONTEXT DER REGULATORIK

Einleitung

Individuelle Datenverarbeitung (IDV) und die sich daraus ergebende Schatten-IT bei Banken stellt nicht nur das IT-Management hinsichtlich IT-Risikocontrolling und IT-Compliance vor besondere Herausforderungen, sondern rückt auch immer stärker in den Fokus der Aufsichtsbehörden. Dieser Beitrag stellt Besonderheiten im Umgang mit IDV dar, ordnet das Thema in den regulatorischen Kontext ein und schließt mit dem Versuch, Methoden zum IDV-Testmanagement aufzuzeigen.

Problemstellung

Im Idealfall werden IT- und Software-Implementierungen von der zuständigen IT-Abteilung eines Kreditinstituts durchgeführt. Insbesondere im Bereich der Softwareentwicklung und durch das immer weiter verbreitete Wissen um Software und Programmierung sind auch Mitarbeiter aus IT-fernen Abteilungen vermehrt in der Lage, Softwareanwendungen zu entwickeln, einzusetzen und zu pflegen. Dieser Sachverhalt begünstigt die Entstehung von Schatten-IT, die sich dem Zugriff, der Überwachung und der Compliance einer zentralen IT-Abteilung weitestgehend entzieht. Aus bankprozessualer Sicht bietet dies Chancen und Risiken zugleich. So ist es durchaus möglich, dass sich aus IDV-Anwendungen im Laufe der Zeit Unternehmensprozesse entwickeln,

die durchaus in einem Wettbewerbsvorteil münden können. Dem gegenüber stehen teils mangelnde DSGVO-Konformität, fehlende Überwachung und Dokumentation sowie Pflege der jeweiligen IDV-Anwendung. So kann aus einem sich über Jahre aufbauenden IDV-Wildwuchs ein ernstzunehmendes operationelles Risiko für die IT-Sicherheit entstehen.

Charakterisierung von Individueller Datenverarbeitung

Unter IDV versteht man Softwareprogramme, die vom Endnutzer bzw. Anwender in den jeweiligen Fachabteilungen entwickelt und gepflegt werden. Dadurch entstehen von den geordneten IT-Prozessen losgelöste Unternehmens- und Geschäftsprozesse, die vergleichsweise schwer zu überwachen sind.

Typische Trägersysteme, die in der Praxis regelmäßig zum Einsatz kommen, sind u.a. SQL-Abfragen, VBA-Anwendungen und Makros, die mit Microsoft Excel und Access ausgeführt werden. Die wahrscheinlich häufigste Motivation der Endanwender, eine IDV-Anwendung zu entwickeln, ist die Schnelligkeit, mit der ein solches Vorhaben realisiert werden kann. Häufig hindern lange Genehmigungs- und Budgetierungsverfahren über die offiziellen internen Instanzen in der Bank eine schnelle und effiziente Abhilfe in den Fachbereichen. Darüber hinaus kommen selbstentwickelte Anwendungen häufig bei Arbeiten zum Einsatz, die mit hohem manuellen Einsatz und/oder Medienbrüchen erledigt und unregelmäßig durchgeführt werden. Vor allem die Datenaggregation für aufsichtliche Meldungen unterliegt fortlaufenden Veränderungen auf Seiten der Datenzulieferer und -Abnehmer. Sobald sich die Fachabteilung mit selbstentwickelten Tools Abhilfe schafft, liegt IDV vor.[1]

Regulatorische Rahmenbedingungen

Die zunehmende Anzahl an IT-Pannen und die weltweit stärker werdende Bedrohung durch Cyberattacken auf Finanzdienstleister hat das Thema IDV verstärkt in den Fokus der internationalen und deutschen Aufsichtsbehörden gerückt. Die Deutsche Bundesbank hat im Jahr 2013 erstmals ihre Anforderungen an den Umgang mit IDV beschrieben.[2] Im Jahr 2017 wurde das Thema in der fünften Novelle der Mindestanforderungen an das Risikomanagement (MaRisk) und mit den

[1] Vgl. Biernat (2019)
[2] Vgl. Deutsche Bundesbank (2013), Anforderungen an individuelle Datenverarbeitung aus aufsichtlicher Sicht

am 06.11.2017 von der Bafin veröffentlichten bankaufsichtlichen Anforderungen an die IT (BAIT) konkretisiert.
Neben den unterschiedlichsten IT-spezifischen Sachverhalten werden in Kapitel 6 des BAIT-Regelwerks explizit das Thema Anwendungsentwicklung angeführt, die auch IDV-Anwendungen mit einschließen. Dies bedingt, dass die Verfügbarkeit, die Integrität, die Vertraulichkeit sowie die Authentizität (VIVA-Prinzip) für alle IT-Systeme und die dazugehörigen Prozesse und Daten gewährleistet sein müssen.[3] Die vier Eckpunkte sind folgerichtig auch von allen im Institut angewendeten (kritischen) IDVs zu erfüllen.[4] Die Anforderungen des AT 7.2 MaRisk gelten auch für die im Institut eingesetzte IDV; Maßstab ist die Kritikalität der unterstützen Geschäftsprozesse und die Bedeutung der einzelnen IDV-Anwendungen für diese Prozesse. Da nicht jede IDV per se als stark risikogefährdend eingestuft werden kann, sind nach erfolgter Identifizierung Risikoklassifizierungen durchzuführen und Schutzbedarfsklassen zu bilden.[5] Alle daraufhin abgeleiteten Maßnahmen zur IT-Risikosteuerung und zur Datensicherheit haben sich am zuvor entwickelten Schutzbedarf zu orientieren. Darüber hinaus ist gem. BAIT Tz. 44 eine revisionssichere und nachvollziehbare Dokumentation des Softwareentwicklungsprozesses anzulegen. Um die Funktionalität und die Qualität der Software sicherzustellen sind geeignete Testverfahren vor dem erstmaligen (Live)-Einsatz anzuwenden. Die Tests sollen neben der Funktionalität auch die Sicherheitskontrollen und die Systemleistungen unter verschiedenen Stressbelastungen einbeziehen.[6]

Implikationen für das IDV und -Testmanagement

Innovationsbestrebungen und agile Unternehmensführung sind im Zuge der zunehmenden Digitalisierung von Geschäftsprozessen und -modellen en vogue. Aus ökonomischer Sicht sind fachabteilungsgetriebene Software-Entwicklungen zu begrüßen, wenngleich damit eine lückenhafte IT-Infrastruktur begünstigt wird, die unter IT-Risikomanagementgesichtspunkten kritisch zu sehen ist. Die Herausforderung im Umgang mit IDV besteht zunächst darin, alle kritischen Anwendungen im Unternehmen zu identifizieren. Die Identifizierung solcher IDV-Anwendungen kann z.B. mit Hilfe von vorformulierten Leitfragen geschehen:

[3] MaRisk (2017), AT 7.2, Tz. 2
[4] MaRik (2017), AT 7.2, Tz. 5
[5] Vgl. BAIT (2018), Tz. 43
[6] Vgl. BAIT (2018), Tz. 41

- Erfolgt die Weiterentwicklung und Pflege der Anwendung im Fachbereich?
- Wird durch die Nutzung der Anwendung eine organisatorische Veränderung im eigenen oder im fremden Fachbereich bedingt?
- Wird die Anwendung regelmäßig genutzt?
- Erfolgt ein Datenaustausch mit anderen Systemen und werden dadurch Abhängigkeiten erzeugt?
- (…)

Die o.g. Leitfragen lassen sich individuell abändern und weiterentwickeln. Die Aufsichtsbehörden haben keine konkreten Methoden hinsichtlich der IDV-Identifizierung vorgeschlagen. Nach erfolgter Identifizierung sind die Anwendungen hinsichtlich ihres Risikogehalts (Schadenshöhe * Eintrittswahrscheinlichkeit) zu clustern. Anwendungen, die keine oder nur eine geringe Geschäftsauswirkung haben (z.B. excelbasierte Urlaubslisten oder Speisepläne), stellen i.d.R. Hilfsmittel dar und sind keine IDV im regulatorischen Kontext.
Anhaltspunkte zur Bestimmung des Risikogehalts können sämtliche Fragestellungen sein, die zur Erfüllung des VIVA-Prinzips beitragen. Darüber hinaus können auch handels- und steuerrechtliche Datenverarbeitung sowie datenschutzrechtliche Aspekte zur Bewertung der Kritikalität herangezogen werden. Ferner ist für alle IDV-Anwendungen die Schadenshöhe und Eintrittswahrscheinlichkeit risikoorientiert einzuschätzen. Auch die Fragen hinsichtlich Notfallplänen und DSGVO-konformen Löschkonzepten sind für jede IDV zu bewerten. Zudem ist zu überprüfen, ob die Anwendung im Notbetrieb zur Verfügung stehen muss und ob sie daher in ein entsprechendes Notfallmanagement-System aufzunehmen ist. Anwendungen mit hohem Risikogewicht sind idealerweise zur Überwachung und Pflege der IT-Abteilung zu unterstellen. Darüber hinaus ist auch für IDV-Anwendungen ein revisionssicheres Testmanagement aufzusetzen, was sämtliche Anforderungen eines professionellen Testmanagements simultan erfüllt.
Erfahrungsgemäß existiert hier ein Gap, da die Anforderungen an ein revisionssicheres Testmanagement nur unzureichend erfüllt werden. Die ordnungsgemäße Dokumentation**,** ein adäquates Testmanagement sowie ein schlüssiges und konsequentes Berechtigungsmanagement sucht man häufig in einer organisch gewachsene Schatten-IT vergebens. Ferner ist eine personelle bzw. organisatorische Trennung zwischen Softwareentwicklung und Softwaretester häufig nicht gegeben, welche

jedoch aus regulatorischer Sicht zwingend erforderlich ist.[7]
Die Konsequenz daraus ist, dass nur eine unzureichende Testabdeckung erreicht wird. Um IDV-Anwendungen im Sinne der regulatorischen Bestimmungen zu testen, kann auf die allgemeingültigen Methoden und Verfahren des Software-Testens (ISO 27000) zurückgegriffen werden. Ein adäquates Testkonzept sollte auf jeden Fall die folgenden Punkte enthalten:

- Beschreibung der Testbasis
- Darlegung der Teststrategie (Testziele Teststufen, Testarten etc.)
- Beschreibung der Testinfrastruktur mit relevanten Schnittstellen,
- Abweichungen von internen IT-Entwicklungsstandards und weiteren Besonderheiten sowie
- Annahmen und Einschränkungen.

Darüber hinaus ist ein Testplan zu erstellen, aus dem sämtliche relevanten Informationen hervorgehen. Dies betrifft in erster Linie Ansprechpartner, die zu nutzende Testinfrastruktur, anzuwendende Methoden und die passende Dokumentation. Aus letzterer muss ersichtlich werden, inwieweit die Anwendung die (fachlichen) Anforderungen erfüllt. Zudem sollten alle verfügbaren Informationen und Erfahrungswerte im Defect-Management festgeschrieben werden.
Beginnend mit dem zugrundeliegenden Fach- und IT-Konzept, kann mit einem Dokumententest gestartet werden. Erste Fehler lassen sich damit gleich zu Beginn des Entwicklungsprozesses aufdecken und Fehlerbehebungskosten reduzieren. Zudem sind logische Testfälle zu definieren, die Informationen über

- das Testobjekt,
- eine ausführliche Testfallbeschreibung,
- die jeweiligen Testschritte,
- Eingaben und
- die erwarteten Ergebnisse enthalten.

Daraus lassen sich konkrete Testfälle ableiten, die auf einer dafür geeigneten Testumgebung durchzuführen sind.
Die Durchführung von Regressionstests ist theoretisch sinnvoll, wenngleich die Durchführung je nach Anwendung individuell abzuwägen ist, da oft eine ausgeglichene Kosten-Nutzen-Relation nicht gegeben ist.

[7] Vgl. BAIT, Tz. 41

Ausblick & Fazit

Um IDV-Anwendungen unter regulatorischen Gesichtspunkten angemessen zu managen, sind grundlegende Entscheidungen in der IT-Strategie im Umgang mit Schatten-IT festzuhalten. Aus ökonomischer Sicht ist es sicherlich zu begrüßen, dass IT-affine Mitarbeiter Eigeninitiative zeigen und Anwendungen selbst schreiben, die für einen effizienteren Arbeitsfluss und geringe Entwicklungskosten sorgen. Um die sich daraus ergebenen Vorteile mit IT-Sicherheitsaspekten zu kombinieren, ist ein offener Umgang mit IDV-Anwendungen zu forcieren, der sich auch in der IT-Strategie des Unternehmens wiederfinden sollte. Im Ergebnis kann so der Zielkonflikt zwischen IT-Sicherheit, Innovationsbestrebungen und agiler Unternehmensführung abgemildert werden. Eine stärkere Zusammenarbeit zwischen IT- und Fachabteilung ist in diesem Zusammenhang unausweichlich.

Der Umgang mit bestehenden IDV-Systemen kann sich dahingehend schwierig gestalten, dass Wissen über die Code-Struktur oder Annahmen des Entwicklers nicht dokumentiert sind und selbst für fachkundige Dritte nicht nachvollziehbar ist. Die damit einhergehenden Risiken einer solchen „Blackbox“ können i.d.R. nur unter sehr hohem Aufwand quantifiziert werden.

Betrachtet man die Bestrebungen der Aufsichtsbehörden, kann man zudem den Eindruck gewinnen, dass die individuelle Datenverarbeitung in den Instituten zukünftig vermehrt mit Anwendungen durchgeführt werden soll, die mit vergleichsweise einfachen Programmiersprachen, wie z.B. Python entwickelt wird. Python gilt als eine sehr leicht lesbare sowie verständliche Programmiersprache und bietet sich daher gut an.

Aus strategischer Perspektive ist es angebracht, seine bestehende IDV-Landschaft zu analysieren und ggf. umzubauen. Diejenigen Prozesse, welche bislang mit Trägersystemen, wie z.B. Excel und/oder Access unterstützt wurden, gilt es überprüfen. In diesem Zusammenhäng ließen sich kritische IDVs durch professionell entwickelte Anwendungen ablösen. Die revisions- und aufsichtlichen Aspekte hinsichtlich Dokumentation und Testing können dort von Anfang an den Entwicklungsprozess begleiten und verringern die Wahrscheinlichkeit der aufsichtlichen Beanstandung.

Wir unterstützen Sie gerne bei der Identifizierung eines konkreten Handlungsbedarfs in Ihren Häusern. Sprechen Sie uns dazu einfach an (info@1plusi.de)!