Benedict Luse,
Benjamin Bogert,
Yannick Ehmann
04/2021

IDV-ANWENDUNGEN – NUR NOCH KURZFRISTIG VON DER AUFSICHT GEDULDET?

Individuelle Daten-verarbeitung (IDV) – Vorteile und Einsatzgebiete

IDV-Anwendungen erfreuen sich vor allem im Finanzsektor großer Beliebtheit. **Einfach, unkompliziert und schnell** sind die Schlagwörter, die vielen auf Anhieb zum Begriff „IDV“ einfallen. Und tatsächlich sind die großen Vorteile von IDV-Anwendungen, dass sie im Vergleich zu komplexen Softwarelösungen deutlich kostengünstiger und zusätzlich viel schneller umsetzbar sind. Für viele Problemstellungen ist es wichtig, dass die Anwendung maßgeschneidert zum Unternehmen passt, was sich mit individuellen Toollösungen sehr gut und effizient realisieren lässt. Beispielsweise sind das Anreichern, Berechnen und Speichern von Daten über IDV-Anwendungen deutlich günstiger und flexibler im Vergleich zu den herkömmlichen Datenbanksystemen und finden deshalb unter anderem in Bereichen wie dem Risikomanagement oder dem Controlling Anwendung. Allen Vorteilen zum Trotz verbergen sich hinter IDV-Anwendungen aber auch Risiken, die nicht zu vernachlässigen sind und aufgrund derer die Aufsicht die Vorschriften in diesem Bereich immer weiter ausweitet.

Bank-aufsichtliche Anforderungen an die IT (BAIT)

Mit dem Rundschreiben 10/2017 (BAIT) hat die Bafin bereits ihre verschärften Anforderungen an die IT-Landschaft der Finanzinstitute deutlich gemacht. IT-Governance und Informationssicherheit spielen keine Nebenrolle, „(…) sondern haben auch für die Aufsicht inzwischen den gleichen Stellenwert, wie die Ausstattung der Institute mit Kapital und Liquidität.“[1] Diesbezüglich achtet die Aufsicht darauf, dass an IDV-Lösungen höchste Anforderungen gestellt werden.

[1] Rundschreiben 10/2017 (BA) - BAIT: Anschreiben an die Verbände

Welche Risiken verbergen sich hinter IDV-Lösungen?

IDV-Lösungen entstehen oft aus Ad-hoc-Lösungen heraus. Hierbei wird häufig das Augenmerk auf eine schnelle und unkomplizierte Umsetzung gelegt, wodurch Themen wie Dokumentation, Test, Wartbarkeit, Sicherheit, Nachvollziehbarkeit oder Nutzerfreundlichkeit mitunter vernachlässigt werden. Sicherheits- und Programmierstandards werden nur selten berücksichtigt und für Dritte ist es oftmals nicht ohne Weiteres möglich, das Programm bzw. den Programmcode zu verstehen, um Anpassungen oder Korrekturen ohne große Risiken vornehmen zu können.

Vorgaben der Bafin

Um solch fehlerhafte Vorgehensweisen zu verhindern, stellt die Bafin im Rundschreiben 10/2017 (BA) wie auch in der Konsultationsfassung zu dessen Novellierung von 2020 klar, dass für die Anwendungsentwicklung angemessene Prozesse festzulegen sind. Diese sollen Vorgaben zur Anforderungsermittlung, zum Entwicklungsziel, zur technischen Umsetzung (inkl. Programmierrichtlinien), zur Qualitätssicherung sowie zu Tests, Abnahme und Freigabe enthalten. Dabei unterstreicht die Bafin zusätzlich, dass unter Anwendungsentwicklungen auch IDV-Lösungen fallen.

Je nach Schutzbedarf sind für die Anwendungsentwicklung weitere Vorkehrungen zu treffen. Darunter wird von der Bafin verstanden, dass für jede Anwendung die **Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten** sichergestellt ist. Beispiele, die in der BAIT für solche Vorkehrungen genannt werden, sind:

- Prüfung der Eingabedaten
- Systemzugangskontrolle
- Benutzerauthentifizierung
- Behandlung von Ausnahmen

Weitere Probleme, welche häufig bei einfachen IDV-Lösungen auftauchen, sind die Möglichkeiten einer **versehentlichen Änderung oder absichtlichen Manipulation** der Anwendung. Gemäß BAIT müssen – abhängig vom Schutzbedarf– Vorkehrungen getroffen werden, die erkennen lassen, ob eine Anwendung versehentlich oder absichtlich verändert wurde.

Unumgänglich für die Entwicklung und den Betrieb einer jeden Anwendung ist eine übersichtliche und für sachkundige Dritte nachvollziehbare **Dokumentation**. Laut BAIT müssen *mindestens* vorhanden sein:

- Anwenderdokumentation
- Technische Systemdokumentation
- Betriebsdokumentation

In Abschnitt 7.11 der BAIT-Konsultationsfassung von 2020 wird außerdem ausführlich auf das Thema **Testen** hingewiesen. Die Bafin schreibt dazu, dass Methodiken für das Testen von Anwendungen vor der erstmaligen Inbetriebnahme sowie nach wesentlichen Änderungen zu definieren und einzuführen sind. Dabei sollen die Testumgebungen zur Durchführung der Abnahmetests im Wesentlichen identisch zur Produktionsumgebung sein. Das Testen an sich und das daraus resultierende Testergebnis sind dabei zu dokumentieren. Tester müssen unabhängig von den Anwendungsentwicklern sein und eine einschlägige Expertise mitbringen. Auch hier gibt die Bafin Punkte an, die bei der **Testdokumentation** mindestens enthalten sein müssen:

- Testfallbeschreibung
- Dokumentation der zugrunde gelegten Parametrisierung des Testfalls
- Testdaten
- erwartetes Testergebnis
- erzieltes Testergebnis
- aus den Tests abgeleiteten Maßnahmen

Die **Ermittlung des Schutzbedarfs** wird in Abschnitt 7.13 der Konsultationsfassung konkretisiert. Hier heißt es, dass ein angemessenes Verfahren zur Klassifizierung bzw. Kategorisierung sowie der Umgang mit den IDV-Anwendungen festzulegen ist. Jede Anwendung ist einer Schutzbedarfsklasse zuzuordnen. Werden dabei die vorher definierten Schutzmaßnahmen eines Programms nicht erfüllt, müssen Nachbesserungen durchgeführt werden. Vor allem bei Anwendungen, bei denen der ermittelte Schutzbedarf die technischen Schutzmöglichkeiten übersteigt, kann es dabei zu Schwierigkeiten kommen.

Um die Vorgaben der von Mitarbeitern entwickelten oder betriebenen Anwendungen zu regeln, schlägt die Bafin die Entwicklung von **IDV-Richtlinien** vor. Außerdem soll ein zentrales Register geführt werden, bei dem ein Mindestmaß an Informationsgehalt vorgegeben wird.[2]

Damit die Prüfungssicherheit der IDV-Landschaft gewährleistet werden kann, empfiehlt sich eine Inventarisierung, auf die im Folgenden eingegangen wird.

Umsetzung der BAIT-Anforderungen

Vor der konkreten Inventarisierung ist die Erstellung von detaillierten **IDV-Richtlinien und Vorgehensmaßnahmen** wichtig. Diese müssen sich an den Vorgaben der BAIT orientieren, damit sichergestellt werden kann, dass die überarbeitete IDV-Landschaft alle regulatorischen Anforderungen erfüllt.

Während der **Inventarisierung** werden zunächst alle IDV-Anwendungen identifiziert. Danach wird für jede Anwendung der Schutzbedarf bzw. das Schutzniveau ermittelt und dokumentiert, damit im nächsten Schritt geeignete Maßnahmen, wie zum Beispiel Zugriffsbeschränkungen oder Automatisierungsgrade, abgeleitet werden können, die dann im dritten Schritt zu implementieren sind.

Im Zuge der Implementierung werden, wie von der Bafin vorgeschrieben, **Testtemplates und Dokumentationen** erstellt. Des Weiteren ist eine sichere Ordnerstruktur mit Zugriffsrestriktionen oder alternativ eine Benutzeroberfläche einzurichten, die das Berechtigungskonzept der Anwender steuert. Letzteres bietet eine sicherere Alternative und ist mit Hilfe von Programmiersprachen wie Python, R, aber auch VBA schnell und effizient umsetzbar. Generell ist für Anwendungen von besonders hohem Schutzbedarf abzuwägen, die Implementierung in den genannten Programmiersprachen umzusetzen, um ein höheres Schutzniveau zu erzielen.

Projektfahrplan prüfungssichere IDV-Landschaft

Um den Weg zu einer prüfungssicheren IDV-Landschaft zu unterstützen, hat sich gemäß unserer Erfahrung aus entsprechenden Beratungsprojekten nachfolgender Projektfahrplan bewährt:

[2] Rundschreiben 10/2017 (BA) in der Fassung von 2020

Fazit

Zusammenfassend lässt sich sagen, dass die Bafin nach wie vor IDV-Lösungen zulässt und in Zukunft auch zulassen wird – dies allerdings unter strengeren Richtlinien und Vorschriften. Ausführliche bankinterne IDV-Richtlinien, die bei der Entwicklung neuer IDV-Lösungen beachtet werden müssen, sind unumgänglich. Außerdem empfiehlt sich dringend eine Inventarisierung der bestehenden IDV-Landschaft, um gegebenenfalls Mängel zu identifizieren und schnellstmöglich auszubessern.

Sollten Sie fachliche Fragen zu einer prüfungssicheren IDV-Landschaft oder Interesse an der Entwicklung gezielter Toollösungen haben, können Sie sich gerne direkt an uns wenden. Wir freuen uns Ihnen mit unserer langjährigen Erfahrung in der Entwicklung von IDV-Lösungen zur Seite zu stehen. Sollten Sie das Thema IDV auch langfristig als relevant für Ihr Haus erachten, so können wir Sie bei der strategischen Aufstellung und Internalisierung, beispielsweise durch unsere zertifizierten ISTQB (International Software Testing Qualifications Board) Schulungen, unterstützen.

Gerne helfen wir Ihnen auch bei der Identifizierung eines konkreten Handlungsbedarfs. Sprechen Sie uns dazu einfach an (info@1plusi.de)!