Martin Mertens

Die Balance wahren: Elemente einer wirksamen IDV-Governance

Die Notwendigkeit, Vorteile und Risiken der individuellen Datenverarbeitung (IDV) in ein Gleichgewicht zu bringen, machen ein geordnetes Verfahren im Umgang mit IDV notwendig. Darauf hat nun auch die Aufsicht reagiert.

WAS HEISST IDV?

IDV ist die Abkürzung für individuelle Datenverarbeitung, häufig wird sie auch als End User Computing (EUC) bezeichnet. Dabei handelt es sich um von Mitarbeitern der Fachbereiche genutzte EDV-Anwendungen, die außerhalb der von der IT betriebenen zentralen Datenverarbeitung (ZDV) liegen, aber Bestandteil eines Geschäfts- oder Steuerungsprozesses sind beziehungsweise einen dokumentierten Geschäftsprozess unterstützen.

Bezüglich Datenschutz und Stabilität der IT-Infrastruktur kann das Schattendasein dieser IDV-Anwendungen schnell zu einem Sicherheitsrisiko für die Unternehmens-IT werden. Eine wirksame IDV-Governance, also ein stringentes Lebenszyklusmanagement von IDV-Anwendungen, ist daher unbedingt erforderlich.

VORTEILE UND RISIKEN VON IDV

Der Einsatz von IDV kann aus gesamtunternehmerischer Sicht durchaus sinnvoll sein. Mitarbeiter nutzen solche Anwendungen, weil IT-Ressourcen fehlen oder diese Tools ihre individuelle Arbeit kostengünstiger und effizienter unterstützen, als es ZDV-Software könnte. Am häufigsten kommen als Plattformen für IDV-Anwendung EXCEL und ACCESS zum Einsatz, wobei nicht jeder Einsatz dieser Software schon in die Kategorie IDV fällt. So ist zum Beispiel eine einmalige Ad-hoc-Auswertung von produktiven Daten noch keine IDV, sehr wohl aber eine EXCEL-Arbeitsmappe, die regelmäßig produktive Daten durch Formeln oder Funktionen verändert oder aus anderen Daten erzeugt. Und zwar auch dann, wenn die veränderten oder erzeugten Daten „nur“ angezeigt werden (Auswertungsfunktionalität). Im günstigsten Fall können damit zwar Geschäftsprozesse beschleunigt und Kosten eingespart werden. Aber während in der zentralen Datenverarbeitung für das Lebenszyklusmanagement der unternehmensinternen Software klar geregelte Prozesse, Werkzeuge und Strukturen zum Einsatz kommen, fehlen diese in der Regel für IDV-Anwendungen. Die Folgen: hohe Intransparenz, das Risiko von Sicherheitslücken und erhebliche Missbrauchsmöglichkeiten.

REGULATORISCHE ANFORDERUNGEN AN IDV

Diese Risiken sind nun auch in den Fokus der Aufsichtsbehörden für Finanzinstitute gerückt. Reagiert hat die Aufsicht mit einer Reihe strenger Anforderungen an das Lebenszyklusmanagement von IDV-Anwendungen. Zwar untersagt sie den Einsatz von IDV nicht per se, fordert allerdings, dass für die IDV im Wesentlichen dieselben Kriterien gelten müssen wie für die ZDV. In den „Mindestanforderungen an das Risikomanagement“ (MaRisk, AT 7.2) vom Oktober 2017 sowie in den im Dezember 2017 von der BaFin veröffentlichten „Bankaufsichtlichen Anforderungen an die IT“ (BAIT, Abschnitt II und Punkte 43 und 44) formuliert die Aufsicht ihre Anforderungen folgendermaßen:

In der IT-Strategie müssen zwingend Aussagen zu den IDV enthalten sein.

Die Vorgaben zur Identifizierung, zur Dokumentation, zu den Programmierrichtlinien und zur Methodik des Testens, zur Schutzbedarfsfeststellung und zum Rezertifizierungsprozess der Berechtigungen müssen in einem Regelwerk, zum Beispiel in einer IDV-Richtlinie, geregelt werden.

Die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität (VIVA-Eigenschaften) der verarbeiteten Daten muss sichergestellt werden und die Protokollierung beziehungsweise Überwachung der IDV-Nutzung nach Maßgabe des Schutzbedarfs erfolgen.

Es müssen Prozesse zur Berechtigungsvergabe und Rezertifizierung unter Wahrung der Funktionstrennung etabliert sowie Entwicklungs-, Test- und Abnahmeprozesse eingerichtet werden.

Eine strikte Trennung von Test- und Produktionsumgebung ist ebenso erforderlich wie eine adäquate Durchführung von IT-Risikomanagement und Betriebsprozessen (zum Beispiel Datensicherungen).

ELEMENTE EINER WIRKSAMEN IDV-GOVERNANCE

Da ein Ignorieren der IDV nicht zielführend und das Verbieten nicht praktikabel ist, müssen Banken geeignete Maßnahmen und Kontrollmechanismen definieren und in einer IDV-Governance festhalten. Die Elemente einer wirksamen IDV-Governance gliedern sich in Strategie, Aufbau- und Ablauforganisation, Werkzeuge und Best Practices:

Die **IDV-Strategie** ist integraler Bestandteil der IT-Strategie und behandelt im Wesentlichen folgende Fragen:

- Unter welchen Bedingungen ist der Einsatz von IDV zulässig?
- Wie wird der Einsatz von IDV konkret gesteuert, wie sehen die Verantwortlichkeiten aus und welche ZDV-Prozesse und -mechanismen werden auch für IDV eingesetzt?
- Welche mittel- und langfristigen Ziele werden im IDV-Bereich verfolgt, um ein angemessenes Gleichgewicht zwischen erzielbarem wirtschaftlichem Nutzen und dafür einzugehendem Risiko zu erhalten?

Für die Regelung der IDV-Zuständigkeiten ist die **Aufbauorganisation** gefordert. Dazu muss ein IDV-Stab (gegebenenfalls eine Einzelperson) installiert werden, der auf Institutsebene für alle übergreifenden Themen wie Richtlinien, Prozesse, Werkzeuge und Best Practices verantwortlich ist.

Auf Fachbereichsebene sind IDV-Verantwortliche für das Portfolio der IDV des Bereichs zuständig. Außerdem genehmigen sie die Erstellung jeder neuen IDV in den Bereichen der Organisation.

Spezielle IDV-Eigner für jede einzelne Anwendung führen jeden Statuswechsel im Lebenszyklus der Anwendung durch, Freigeber (beide inklusive Stellvertreter) geben jeden Statuswechsel im Lebenszyklus frei.

Die **Ablauforganisation** muss durch definierte Prozesse sicherstellen, dass die Regelungen der IDV-Governance wirksam umgesetzt werden. Dazu definiert und installiert sie einen Erstellungs- beziehungsweise Änderungs- sowie einen Testprozess für die IDV. Dabei müssen im Testprozess ab dem Schutzbedarf „hoch“ besondere Vorgaben eingehalten werden, wie zum Beispiel keine Personalunion von Entwickler, Tester und Freigeber.

Betriebsprozesse regeln den Umgang mit der IDV, insbesondere eine verpflichtende regelmäßige Datensicherung ab der Schutzbedarfsstufe „hoch“.

Der IDV-Zugriffsschutz (Identity & Access Management = IAM) muss im Rahmen der IAM-Prozesse und mittels der IAM-Werkzeuge der ZDV abgewickelt werden, auch bezüglich der Funktionstrennung.

Die **IDV-Werkzeuge** umfassen zwingend ein zentrales IDV-Inventar für Versionsführung und Metadatenpflege für jede IDV, beispielsweise eine SharePoint-Lösung. Optional beziehungsweise bei Bedarf – wenn zum Beispiel Befunde von Revision oder BaFin dies erforderlich machen – ist ein Scan-Werkzeug mit Add-in zur Protokollierung der Nutzung von EXCEL/ACCESS und Musteranalyse zur Identifikation potenzieller IDV-Anwendungen erforderlich. ■

Mit den folgenden Best Practices kann die Handhabung von IDV-Anwendungen erleichtert und für mehr Transparenz gesorgt werden:

- Für jede IDV-Anwendung werden Schutzbedarfsanalyse und Schutzniveaufeststellung analog zur ZDV durchgeführt.
- Die Ablage von IDV-Anwendungen erfolgt ausschließlich in Ordnern auf dafür vorgesehenen zentralen Laufwerken. Die Zugriffsberechtigungen für diese Ordner werden restriktiv gehandhabt und regulär mittels der ZDV-IAM-Prozesse vergeben.
- Der Umfang und die Inhalte der Dokumentation (zum Beispiel Sicherheitskonzept) werden vom Schutzbedarf abhängig gemacht.
- Das Erstellen und der Betrieb von IDV-Anwendungen werden durch entsprechende Regeln auf das sinnvolle Minimum eingeschränkt. Das kann zum Beispiel eine Begründungspflicht für IDV-Anwendungen sowie eine regelmäßige Überprüfung der Notwendigkeit des Einsatzes jeder IDV-Software mit Schutzbedarfsstufe „hoch“ oder „sehr hoch“ sein.
- Die wesentlichen Bereiche der Erstellung für VBA beziehungsweise EXCEL/ACCESS werden in Programmierrichtlinien geregelt.

Ansprechpartner:

Center of Competence
Software
Engineering

Martin Mertens
Principal IT Consultant
martin.mertens@msg-gillardon.de