VAIT UND IT-RISIKOMANAGEMENT IN DER INDIVIDUELLEN DATENVERARBEITUNG

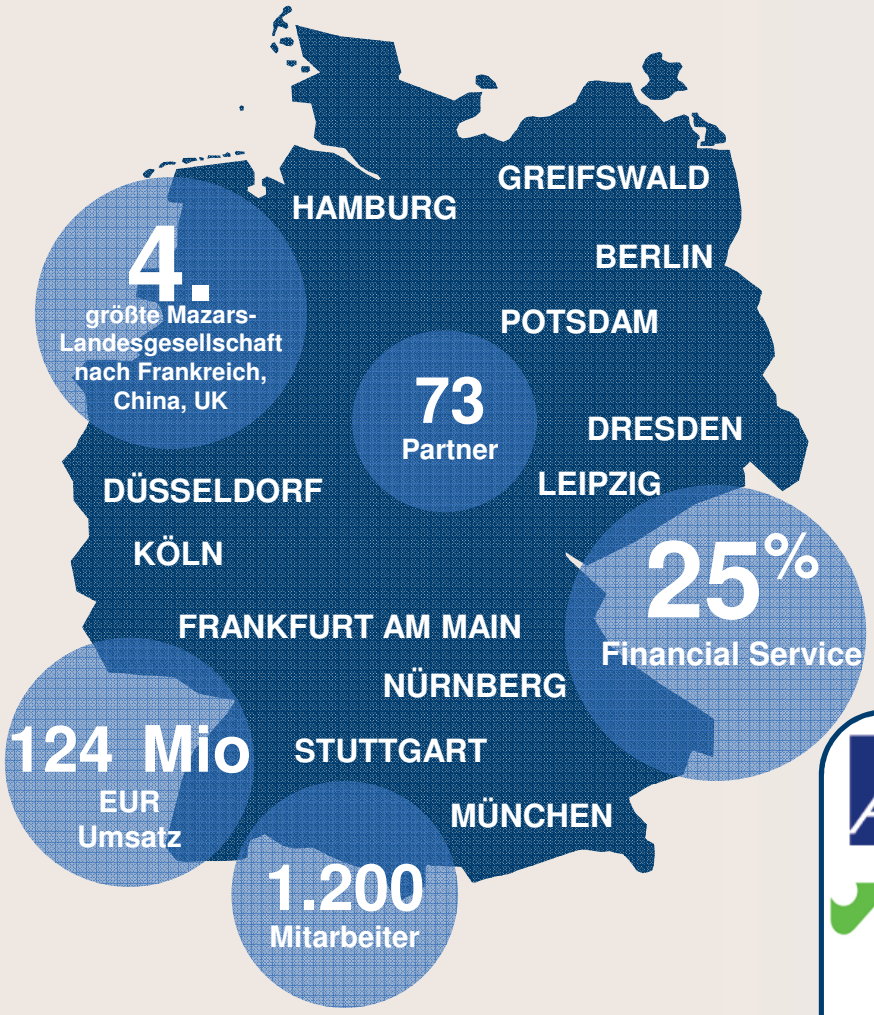
Ralf Engelshove, Detlef Lochmann

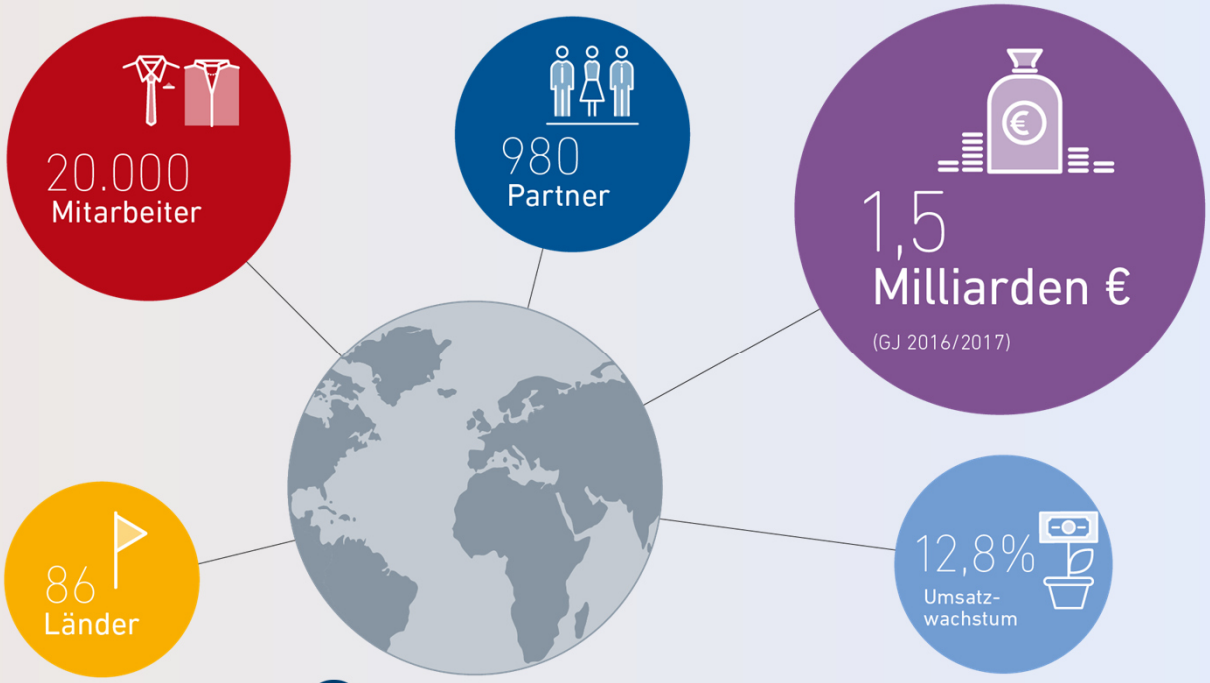
Düsseldorf, 07. März 2018

MAZARS

Roever Broenner Susat Mazars

VORSTELLUNG MAZARS





MAZARS
Roever Broenner Susat Mazars

AGENDA

Ralf Engelshove
Partner

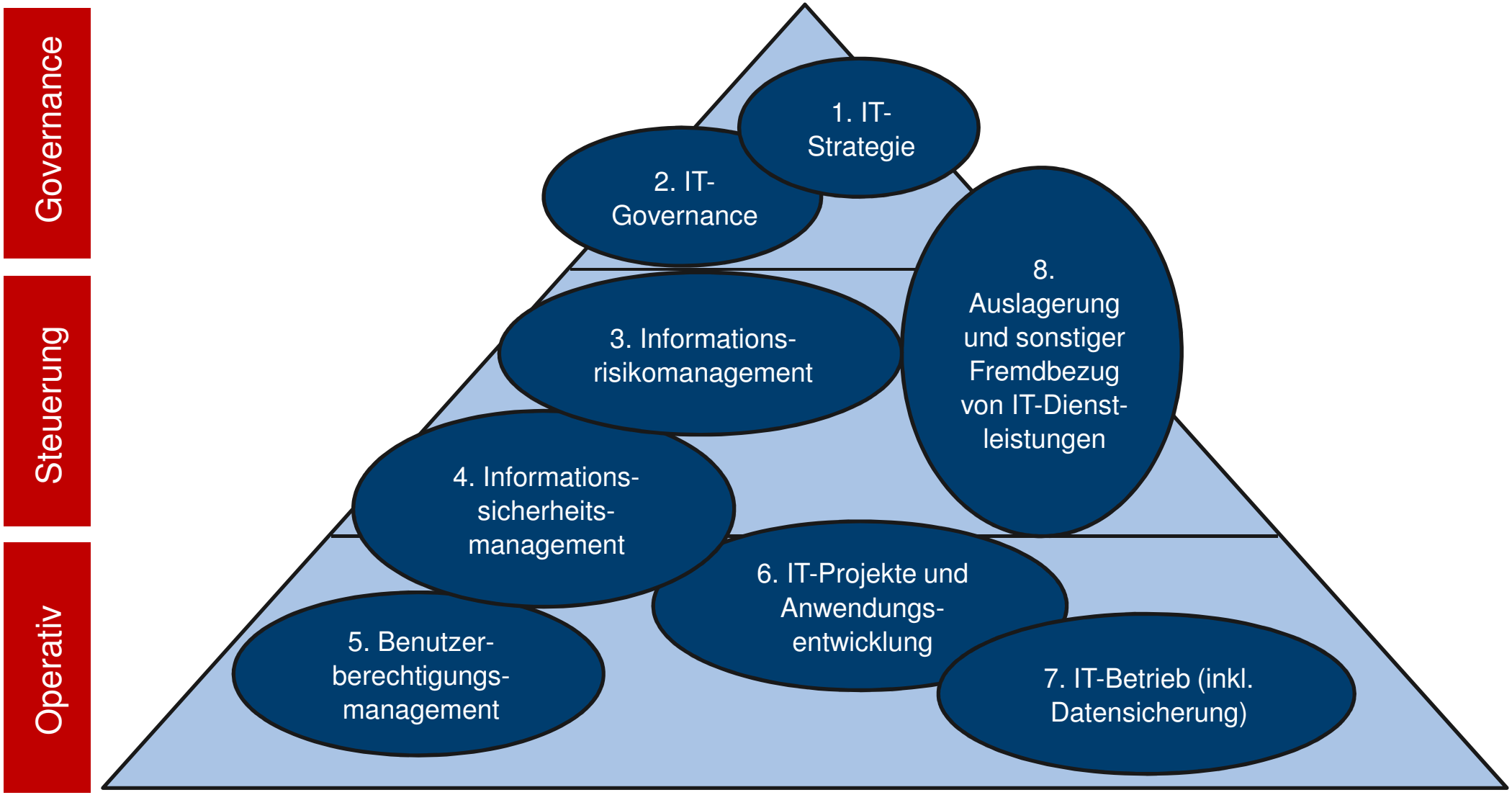
Detlef Lochmann
Director

1. Überblick Aufsichtsrechtliche Anforderungen an die IT
2. Handlungsfelder IDV Risikomanagement
3. Schnittmenge Datenqualität Solvency II
4. Praxiserfahrungen

AUSGANGSLAGE

- **BaFin Abfrage 08/2017:** „Cybersicherheit bei Auslagerungen und individuelle Datenverarbeitung“
- **Aufsichtsrechtliche Anforderungen an die IT für Versicherer (VAIT)**
  - 1. Entwurf v. 06.11.2017, Finalisierung in Q2 2018 geplant (Stand Nov. 2017)
  - Anwendungsbereich: beaufsichtigte Unternehmen (§ 1 Abs. 1 VAG). Ausgenommen Zweckgesellschaften (§ 168 VAG) und Sicherungsfonds (§ 223 VAG)
  - Konkretisierung § 23 Abs. 1 VAG (Geschäftsorganisation) und für SII-Versicherer MaGo R 2/2017
  - Keine abschließende Regelung: zusätzlich gängige Standards (IT-Grundschutzkataloge BSI, ISO/IEC2700x u.ä.)
- **Blick in andere regulierte Branchen**
  - Rundschreiben 10/2017 (BA) - Bankaufsichtliche Anforderungen an die IT (BAIT)
  - Pharma- und Arzneimittelindustrie: European Medicines Agency (EMA): EU Good manufacturing practice (GMP) Leitfaden (Kap.4, Annex 11)
  - BSI-Gesetz/BSI-Kritisverordnung (2016/2017) für Sektoren: Energie, Wasser, Ernährung, IT & Telekommunikation, Gesundheit, Finanz- und Versicherungswesen, Transport & Verkehr („Kritische Infrastrukturen für ein funktionierendes Gemeinwesen“)

ÜBERBLICK DER VAIT-THEMEN



Quelle: BaFin Darstellung zu BAIT

WAS SIND INDIVIDUELLE ANWENDUNGEN ?

Definition, Merkmale

- Durch **Endanwender (Fachbereiche) erstellte Anwendungen** :
  - Programme in einer Programmiersprache
  - Nutzung einer Programmiersprache in einer Anwendungssoftware
- “End User Computing (EUC)”, “End User Developed Applications (EUDA)”.
- Durchlaufen keinen standardisierten Anwendungsentwicklungsprozess einer IT-Abteilung
- Zielsetzung: ad hoc oder regelmäßig auftretenden Informationsaufbereitung, Verarbeitungshilfen u.ä.

Beispiele aus dem Aktuar-Umfeld:

- JAVA-Programme (z.B. BSM)
- MS-Excel, MS-Access, VBA-Markos etc.
- Aktuarielle Modellierungssoftware (Prophet, Igloo, ReMetrica etc.)
- …

KOMPENDIUM

„*LESEN* IST *DENKEN MIT FREMDEM GEHIRN*“ (JORGE LUIS BORGES)

Tz.	im VAIT-Entwurf mit Bezug zu IDV
2	**IT Strategie**: Aussagen zu in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hard- und Softwarekomponente)
42	**Anwendungsentwicklung/IT Projekte: „Tz. 13, 14, 17 und 41 sind auch beim Einsatz von durch die Fachbereiche selbst entwickelten Anwendungen“**…“entsprechend der Kritikalität der unterstützten Geschäftsprozesse und der Bedeutung der Anwendungen für diese Prozesse zu beachten. Die Festlegung von Maßnahmen zur Sicherstellung der Datensicherheit hat sich am Schutzbedarf der verarbeiteten Daten zu orientieren“
13	**Governance**: „Umfang und Qualität der technisch-organisatorischen Ausstattung haben sich am Risikoprofil zu orientieren.
14	Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen die **Integrität**, die **Verfügbarkeit**, die **Authentizität** sowie die **Vertraulichkeit** der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen, insbesondere sind Prozesse für eine **angemessene Berechtigungsvergabe** einzurichten“……“Die Eignung der IT-Systeme und der zugehörigen Prozesse ist **regelmäßig** von den fachlich und technisch **zuständigen Mitarbeitern zu überprüfen**.“
17	Die **Überwachungs- und Steuerungsprozesse** haben insbesondere die Festlegung von IT-Risikokriterien, die Identifikation von IT-Risiken, die Festlegung des Schutzbedarfs, daraus abgeleitete Schutzmaßnahmen für den IT-Betrieb sowie die Festlegung von Maßnahmen zur Risikobehandlung der verbliebenen Restrisiken zu umfassen.
41	„Die IT-Systeme sind **vor ihrem erstmaligen Einsatz und nach wesentlichen Veränderungen zu testen** und von den fachlich sowie auch von den technisch zuständigen Mitarbeitern **abzunehmen**. Hierfür ist ein **Regelprozess der Entwicklung, des Testens, der Freigabe und der Implementierung in die Produktionsprozesse** zu etablieren. Produktions- und Testumgebung sind dabei grundsätzlich voneinander zu trennen.“
54	Ein **angemessenes Verfahren für die Klassifizierung** / Kategorisierung (Schutzbedarfsklasse) und den **Umgang** mit den von Endbenutzern des Fachbereichs entwickelten oder betriebenen Anwendungen **ist festzulegen**
55	Die **Vorgaben zur Identifizierung aller von Endbenutzern des Fachbereichs** entwickelten oder betriebenen Anwendungen, zur Dokumentation, zu den Programmierrichtlinien und zur Methodik des Testens dieser Anwendungen, zur Schutzbedarfsfeststellung und zum Rezertifizierungsprozess der Berechtigungen sind zu regeln (z.B. in einer **IDV-Richtlinie)**

HANDLUNGSFELDER RISIKOMANAGEMENT IDV
ÜBERBLICK

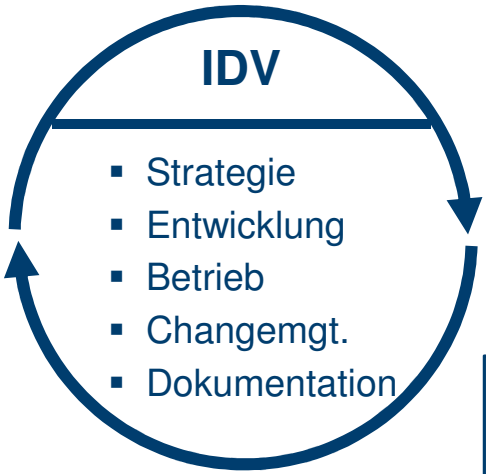
IDV-Richtlinie

Standardsetting für..

- IT-Strategie: Teil IDV
- Festlegung Verantwortlichkeiten
- Aufgabenabgrenzung (IT-, Fachabt.)
- Anleitung Programmierung
- Anleitung Qualitätssicherung
- Anleitung zur Dokumentation
- Schutzbedarfsklassifizierung

Entwicklungsstandards

- Programmänderungsverfahren
- Verfahrensdokumentation
- Zugriffsschutz
- Programmierrichtlinien
- Test- und Freigabeverfahren
- Versionierung



Inventarisierung IDV

- Erstinventur
- Klassifizierung Schutzbedarf
- Permanente oder periodische Aktualisierung

Betriebsstandards

- Trennung von Test und Produktion
- Benutzerberechtigungsmanagement
- Automatisierte Verarbeitungen
- Schnittstellenmanagement
- IT-Kontrollen
- Archivierung von Ergebnissen

MAZARS
Roever Broenner Susat Mazars

2.

Handlungsfelder IDV Risikomanagement

HANDLUNGSFELDER RISIKOMANAGEMENT IDV
STANDARDSETTING

IT Strategie (VAIT Tz. 1-5)

Wer: Vorstand, Aufsichtsgremium zur Kenntnis

Was: Mindestinhalte sind:

- ¬ Strategische Entwicklung der IT-Aufbau -und Ablauforganisation (inkl. “Outsourcing”)
- ¬ An welche gängigen Standards orientiert sich das Unternehmen?
- ¬ Zuständigkeiten und Einbindung der IT-Sicherheit in die Organisation
- ¬ Ausrichtung der IT-Architektur
- ¬ Aussagen zum Notfallmanagement
- » ¬ Aussagen zu den in den Fachbereichen betriebenen bzw. entwickelten IT Systemen « (Hard- und Software)

→ **Handlungsfelder:**

- ¬ Aufnahme von IT-Aussagen in die Geschäftsstrategie; Integration in den Strategieprozess
- ¬ Überprüfung von bestehenden IT-Strategieprozessen und -aussagen auf Mindestinhalte. In der Praxis ist IDV häufig (bislang) nicht Bestandteil der dokumentierten IT-Strategie

.

MAZARS
Roever Broenner Susat Mazars

HANDLUNGSFELDER RISIKOMANAGEMENT IDV
STANDARDSETTING

IDV Richtlinie (VAIT Tz. 55)

Wer: heute i.d.R. IT Abteilung

besser Risiko-, IT-Sicherheits- oder Compliance Management und IT beratend

Was: Vorgaben zur:

- Identifizierung
- Dokumentation
- Programmierrichtlinie
- Testmethodik
- Schutzbedarfsfeststellung
- Zugriffsschutz
- Rezertifizierungsprozess

Bsp. Gliederung	
1	Ziele
2	Definitionen
3	Verantwortliche und Beteiligte
5	Prozesse
5.1	Zugriffsschutz
5.2	Kritikalität
5.3	Entwicklung und Anpassung
5.4	Design Excelsheets u.Qualität Programmcode
5.5	Implementierung von Kontrollen
5.6	Archivierung Berichte/Ergebnis
6	Kommunikation und Berichtswesen
7	Verteiler, Verweisverzeichnis, Änderungshistorie

HANDLUNGSFELDER RISIKOMANAGEMENT IDV
INVENTARISIERUNG DER IDV

- **Zielsetzung**
  - VAIT (Tz. 57) erwartet für alle Komponenten der IT Systeme eine Inventur/Bestandsangaben, unabhängig davon, ob in „Hoheit“ der IT oder der Fachabteilung
  - Überblick, Vermeidung Redundanzen

- **Zentrales Register aller betriebenen IDV Anwendungen** (VAIT-Entwurf Tz. 55):
  - Name und Zweck der Anwendung
  - Versionierung, Datumsangabe
  - Fremd- oder Eigenentwicklung
  - Fachverantwortlicher Mitarbeiter & technisch verantwortlicher Mitarbeiter
  - Verwendete Technologie
  - Risikoklassifizierung und die daraus abgeleiteten Schutzmaßnahmen

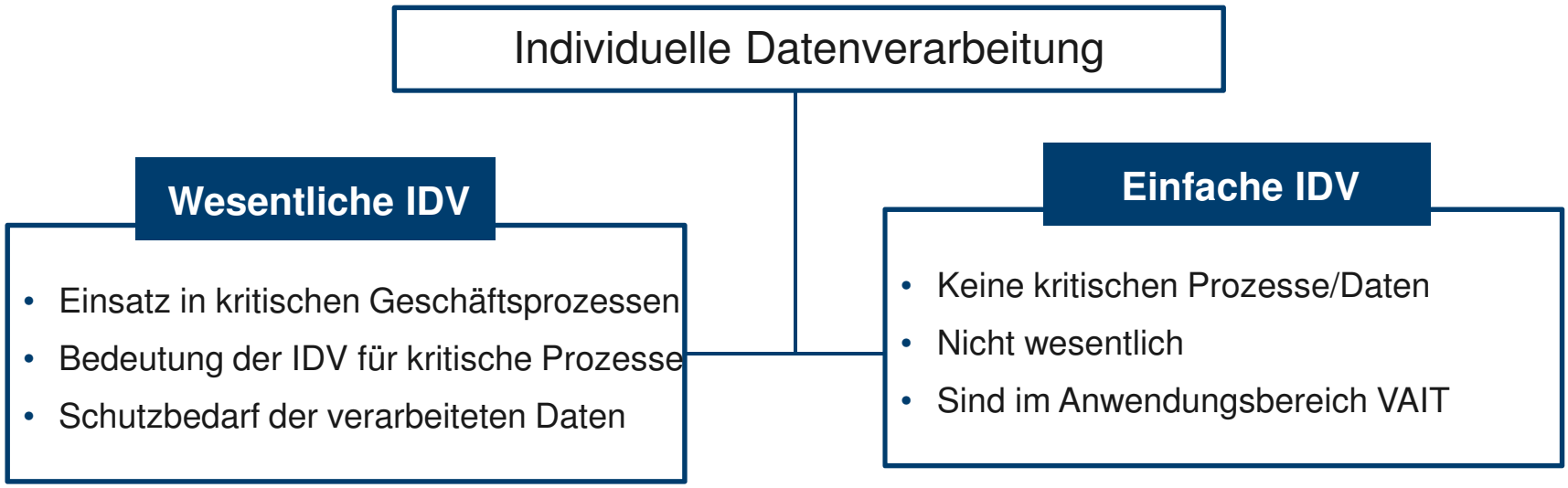
» VAIT sieht eine Inventarisierung aller IDV-Anwendungen, unabhängig von der Kritikalität, vor. Aber nicht jedes „Spread sheet“ ist automatisch IDV. Die Abgrenzungsverantwortung liegt i.d.R. beim Fachbereich «

INVENTARISIERUNG DER IDV
WAS SIND KRITISCHE IDV ANWENDUNGEN?

VAIT-Entwurf Tz 42 u. Tz 54

Tz. 13, 14, 17 und 41 sind auch beim Einsatz von durch die **Fachbereiche selbst entwickelten Anwendungen (IDV)** entsprechend der **Kritikalität der unterstützten Geschäftsprozesse** und der **Bedeutung der Anwendungen für diese Prozesse** zu beachten. Die **Festlegung von Maßnahmen zur Sicherstellung der Datensicherheit** hat sich am **Schutzbedarf der verarbeiteten Daten** zu orientieren.

Ein **angemessenes Verfahren für die Klassifizierung/Kategorisierung (Schutzbedarfsklasse)** und den **Umgang** mit den von Endbenutzern des Fachbereichs entwickelten oder betriebenen Anwendungen ist **festzulegen**.



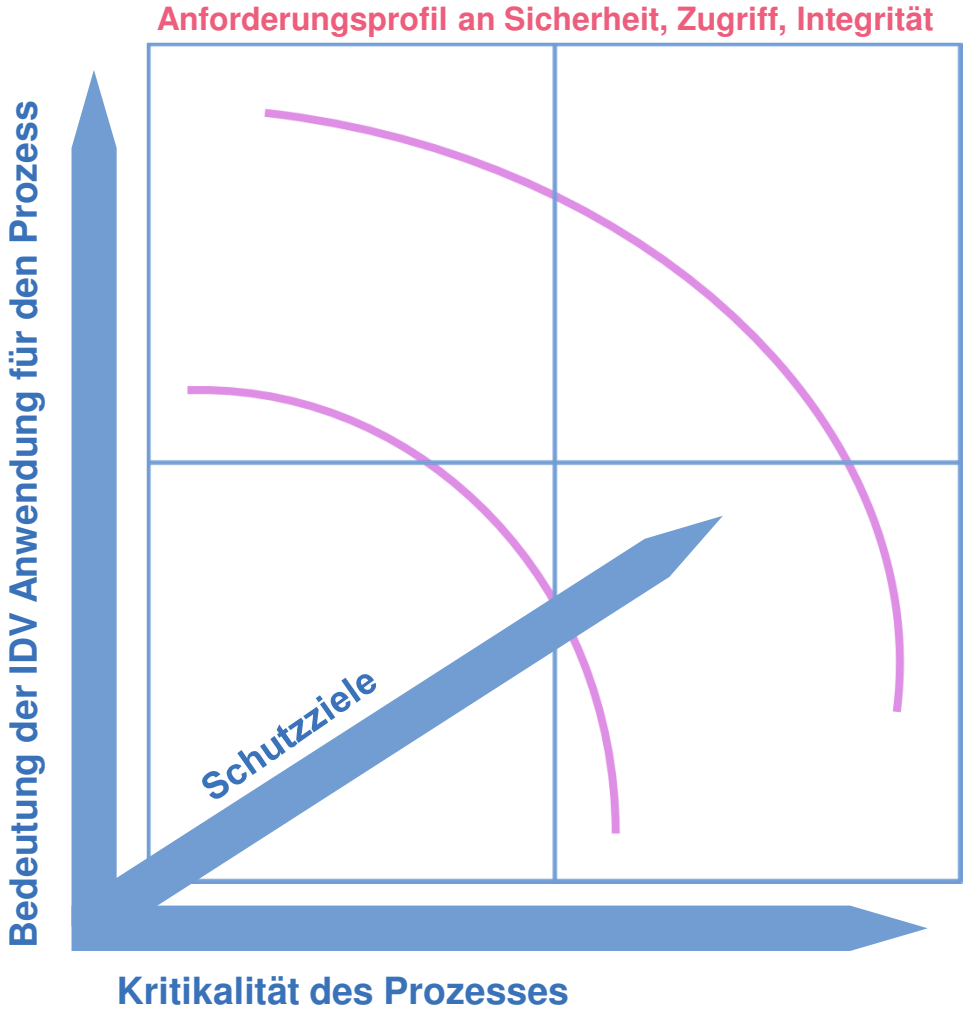
INVENTARISIERUNG IDV
EINORDNUNG IDV IN EINE SCHUTZKLASSE

Die Einordnung in eine „Schutzklasse“ ist abhängig von

- Prozesskritikalität & Bedeutung der Anwendung
- Schutzziele (VAIT Tz. 20)
  - Integrität: „Korrekte Daten, korrekte Funktionsweise“
  - Verfügbarkeit: „Betriebsbereit, wenn gebraucht“
  - Vertraulichkeit: „kein unautorisierter Zugang“
  - Authentizität: „Zuordnung Daten zum Ursprung“
- Klassifizierung muss nachvollziehbar sein
- Turnusmäßige Überprüfung

Erfahrungen aus der Praxis

- fehlender „revisionssicherer“ Nachvollzug
- Der hohe „Schutzbedarf“ kritischer Prozesse kann das Sollprofil der technischen Möglichkeiten übersteigen.



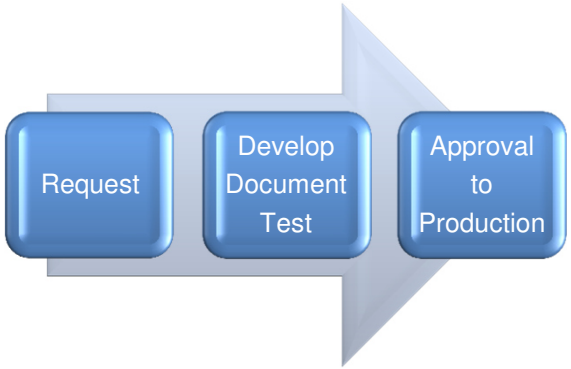
INVENTARISIERUNG DER IDV
WAS SIND INDIZIEN FÜR KRITISCHE GESCHÄFTSPROZESSE/IDV?

- **Einsatz in Kernprozessen**
  - Katalog BSI-KritisV: **Vertragsverwaltungs-, Leistungs- und Exkassosysteme**
  - Prozesse mit Kunden (Vertrieb)
  - Prozesse für **gesetzliche und regulatorische Zwecke** (Rechnungslegung, Steuern, Risikomanagement, Aufsicht etc.)
  - Prozesse in **Schlüsselfunktionen** (VMF, uRCF, IR, CMF, evtl. andere)
- **Entscheidungsrelevanz**
  - Geschäftsprozess liefert Informationen für **wesentliche Managemententscheidungen** (Vorstand, Aufsichtsrat, Risikoausschuss, Anlageausschuss, etc.).
- **Liefert Informationen an externe Prüfer**
  - Wirtschaftsprüfer
  - Betriebsprüfungen: Steuer, Sozialversicherungsträger, etc.
- **Nutzung, Frequenz, Komplexität**
  - Hohe Benutzeranzahl?
  - Große Datenvolumen oder hohe Komplexität?
  - IDV ist eine Kernanwendung in dem Prozess

ENTWICKLUNGSSTANDARDS
PROGRAMMÄNDERUNGSVERFAHREN

- Programmänderungsverfahren
  - Anfrage- fachliche und technische Anforderung
  - Technische Umsetzung über Test und Freigabeverfahren zur Produktivsetzung
  - Fortschreibung bis zur Produktivsetzung und bei späteren Änderungen
  - Versionierung
  - zuzüglich Anwenderdokumentation
  - zuzüglich Schutzbedarfsfeststellung

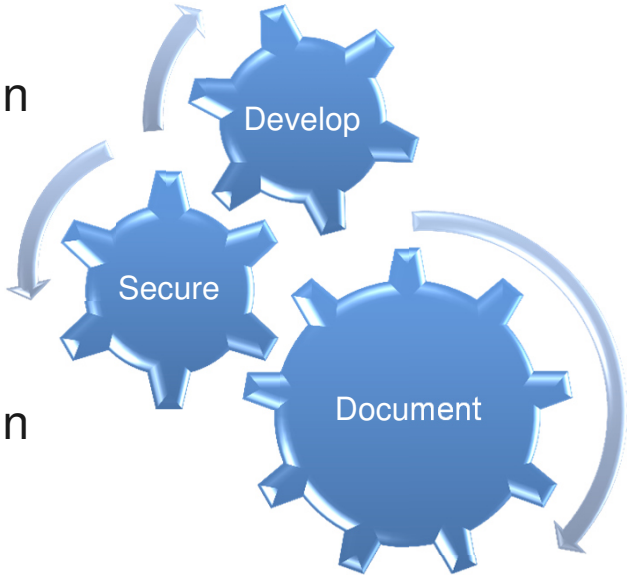
⇒ Wesentliche Bestandteile der Verfahrensdokumentation



- Fachliche Anforderung enthält u.a.
  - Grundlagen der Anforderung, z.B. Gesetz, Aufsicht, Intern
  - Die Formeln für Berechnungen mit Erläuterung
  - Spezifikation der Inputdaten – Herkunft, Selektion, Zeitpunkt
  - Spezifikation des Outputs – Adressaten, Weiterverarbeitung, Zeitpunkte

ENTWICKLUNGSSTANDARDS
PROGRAMMIERRICHTLINIE

- Programmierrichtlinie
  - Genutzte Programmiersprachen, Tools, Entwicklungsumgebung, Versionsverwaltung
  - Bezeichnungen für Variablen, Prozeduren, Programm- und Dateinamen
  - Funktionen und Sprachelemente – bevorzugt – unerwünscht
  - Inline Dokumentation
  - Trennung / Schutz von Eingabe- und Ausgabedaten, Formeln
  - Plausibilitäts- und Fehlerprüfungen, Auswahllisten etc.
  - Protokollierungen

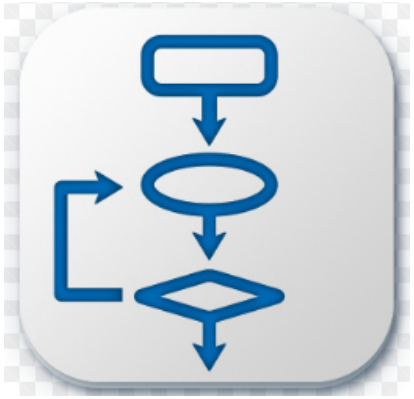


- Zugriffsschutz in der IDV selbst
  - Trennung / Schutz von Eingabe- und Ausgabedaten, Formeln
  - Zellschutz, Passwort für Änderung und Anzeige
  - Schutz des Quellcodes

- Weitere Ebenen CITRIX, Netzwerk, z.B. Active Directory Service (ADS), sind in den Anforderungen für den Betrieb festzulegen.

ENTWICKLUNGSSTANDARDS
TEST- UND FREIGABEVERFAHREN

- Test- und Freigabeverfahren
  - ¬ Trennung (Entwicklung), Test und Produktion
  - ¬ Testplan, -fälle und -ergebnisse
    - – Welche Version wurde getestet?
    - – Was wurde, von wem, wann mit welchem Ergebnis getestet?
    - – Wie wurden identifizierte Fehler behoben und nachgetestet?

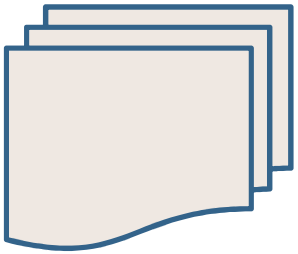


- Regressionstests bei Änderungen
- Der Entwickler testet und stellt nach erfolgreichen Test die IDV für den Fachbereich bereit.

! Test im 4-Augen-Prinzip: Ein anderer fachlicher Mitarbeiter testet und gibt frei.

- Ein regelmäßiger - zumeist jährlicher - Formelreview im 4-Augen Prinzip mit Nachweis ist Bestandteil des Betriebs von IDV

ENTWICKLUNGSSTANDARDS
VERSIONIERUNG



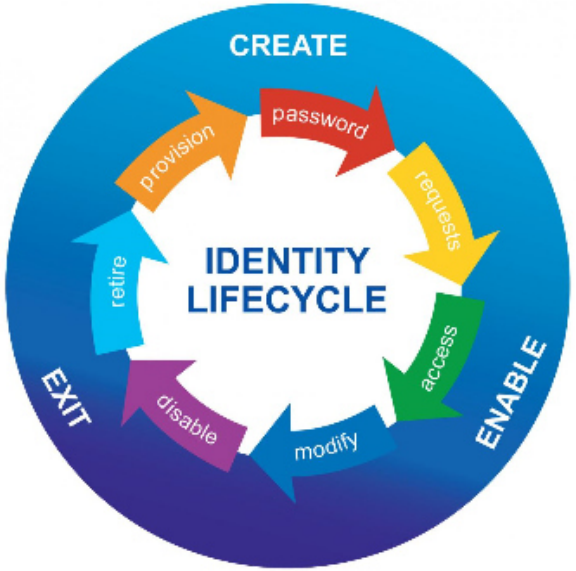
- Versionsverwaltung
  - Über Tools, beispielsweise über Concurrent Versions System (*CVS)*
  - Über Dateinamen – fortlaufende Nummern und Datum
  - Auch während der Entwicklung – spätestens die für den Abnahmetest bereitgestellte Version muss eindeutig benannt sein
  - Die Version sollte idealerweise in der Anwendung und im Output erkennbar sein.

- Stichwort Programmidentität
  - Resultiert aus Anforderung, Dokumentation, Test, Freigabe, Produktivsetzung einer Version
  - Der Test weist die Funktionalität gemäß Anforderung und Dokumentation nach
  - Nachweis über die in einem Zeitraum genutzten Verarbeitungsregeln

! Aufbewahrungspflichtig

BETRIEBSSTANDARDS
BENUTZERBERECHTIGUNGSMANAGEMENT

- Benutzer- und Berechtigungsmanagement
  - ¬ Berechtigungskonzept resultiert aus der Anforderung
    - – Wer darf die IDV ändern, anwenden, nur einsehen
    - – Wer ist der Adressat des Output
- Änderungen im laufenden Betrieb
  - ¬ Austritte und Aufgabenänderungen
  - ¬ Neue Benutzer



- Verantwortungen für Beantragung, Autorisierung und Durchführung => Nachweise.
- Regelmäßiger Review von Benutzern und Zugriffsrechten => Nachweise
- Einrichtungen auf Netzwerk / ADS- Ebene

BETRIEBSSTANDARDS
AUTOMATISIERTE VERARBEITUNGEN

- Anwendungsfelder
  - ¬ Datenbeschaffung oder –bereitstellung
  - ¬ IDV selbst

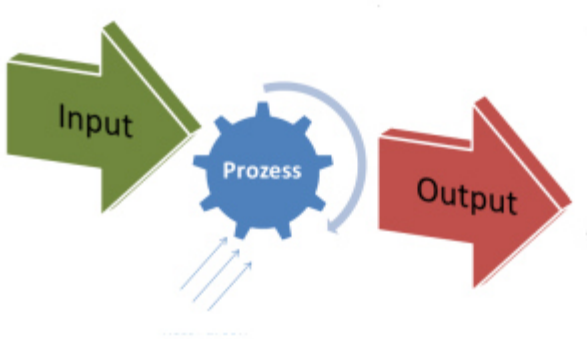
- Dokumentation im Sinne der Beschreibung der automatisierten Verarbeitung
  - ¬ Inklusive Fehlererkennung, -meldung und –behebung => Nachweise über tatsächliche Vorgänge.

- Änderungen in der automatisierten Verarbeitung selbst – Verantwortungen für Antrag, Autorisierung, Durchführung => Nachweis

BETRIEBSSTANDARDS
SCHNITTSTELLENMANAGEMENT

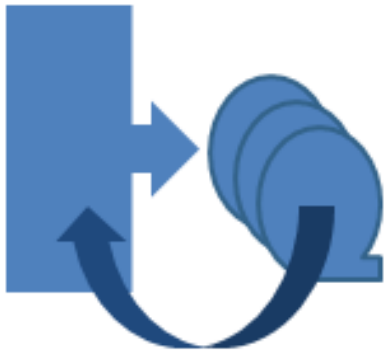
- Input
  - Herkunft, Selektion, Zeitpunkt, weitere Kriterien
  - Kriterien, an denen die Vollständigkeit und Richtigkeit der Input Daten kontrolliert wird
  - Nachweise über die Kontrolle
- Bereitstellung von Daten mit geringer Änderungshäufigkeit
  - Quittung, dass Daten nicht geändert wurden (aus Herkunftssystem oder durch Versender)

- Änderbarkeit von Input Daten
  - Schutz vor Änderungen, z.B. über ADS
  - Erstellen einer schreibgeschützten Kopie
  - Nachweis über ggf. erforderliche Änderungen
- Schutz vor mehrfachem Einlesen
  - Verarbeitete Datei separat abspeichern
  - Input-Dateinamen mit Datum / Zeitstempel
  - Warnung oder Sperren beim Einlesen der Daten in die IDV



BETRIEBSSTANDARDS
IT-KONTROLLEN- VERFÜGBARBKEIT

- Berücksichtigung der IDV
  - Business Impact Analyse (BIA)
  - Business Continuity Plan (BCP)
  - Disaster Recovery Plan (DRP)
  - Back-up- und Restore-Verfahren



- Bedarfsweise
  - Einbindung der relevanten IT Ressourcen in das zentrale Monitoring
  - Rollbackverfahren, um nach einer Rücksicherung über die Logs den Datenverlust zu verringern

- Rücksicherungstests (Restore) idealerweise jährlich, zumindest aber bei der Ersteinrichtung und bei Änderungen (des Dateisystems), der Speicher- oder Backup-Komponenten oder deren Parametrisierung (nachweislich) durchführen.

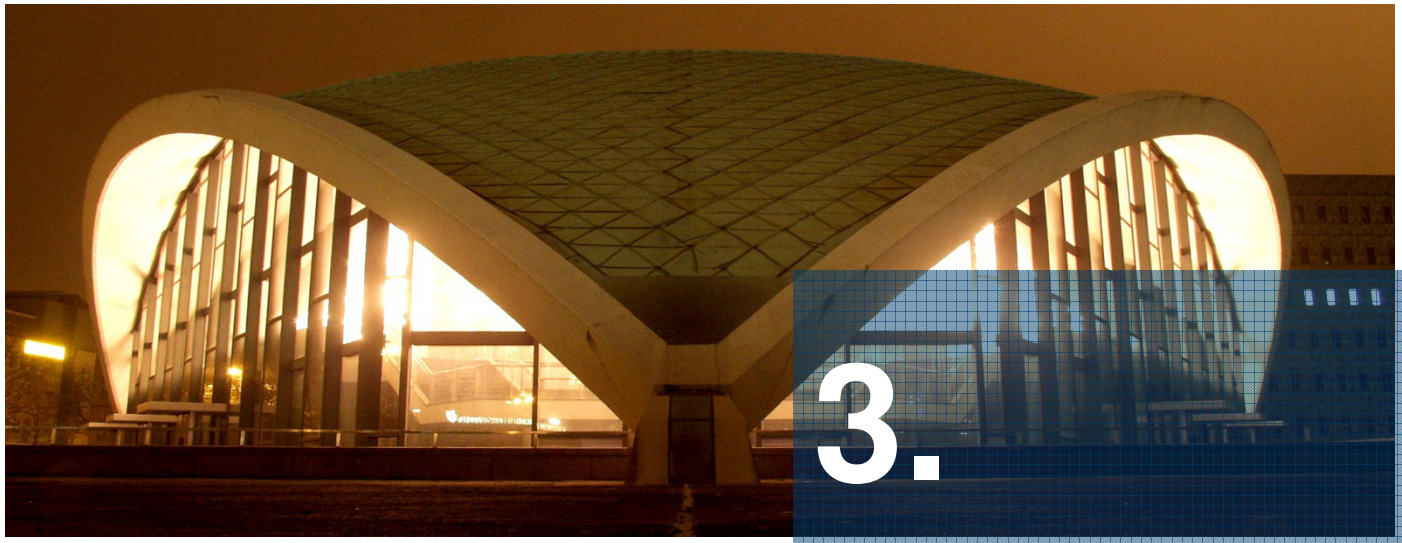
BETRIEBSSTANDARDS
ARCHIVIERUNG VON ERGEBNISSEN

- Als Grundregel gilt: Der Output / die Ergebnisse sind je Erstellung eindeutig im Sinne einer Version zu bezeichnen, beispielsweise über einen Datums- und Zeitstempel oder mit Datum und fortlaufender Nummer.

- Die Ergebnisse sind unveränderbar zu speichern und aufzubewahren.

- Grundformen (Beispiele)

  - Jedes Ergebnis wird in einer Datei gespeichert
  - Eine Datei wird über einen Zeitraum fortgeschrieben und enthält die vorherigen Ergebnisse
  - Je Erstellung wird das vorherige Ergebnisse überschrieben.

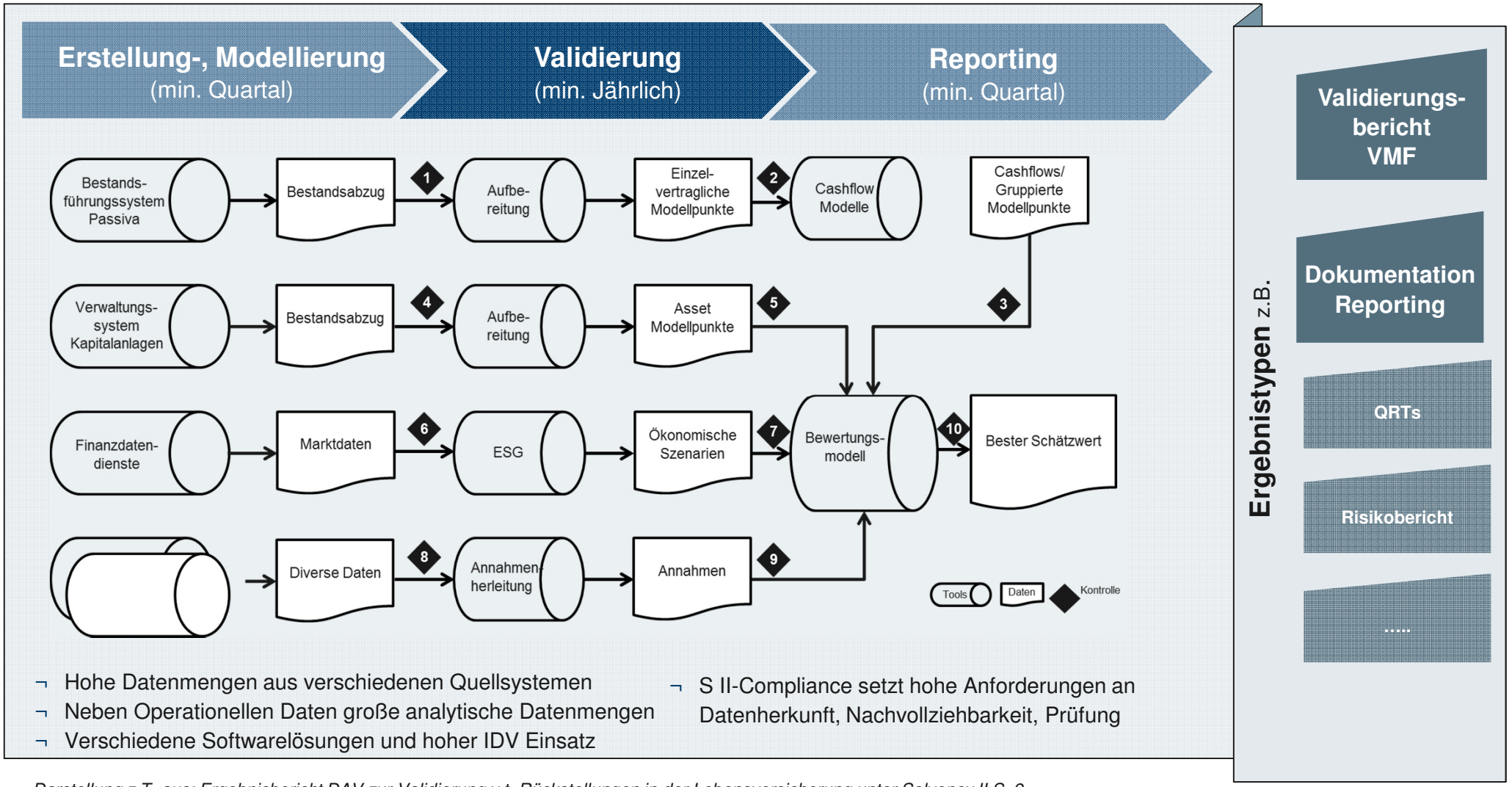


3.

Schnittmenge Datenqualität Solvency II

IDV RELEVANZ FÜR AKTUARIELLE PROZESSE SII

BEISPIEL BEST ESTIMATE LEBEN



- Hohe Datenmengen aus verschiedenen Quellsystemen
- Neben Operationellen Daten große analytische Datenmengen
- Verschiedene Softwarelösungen und hoher IDV Einsatz
- S II-Compliance setzt hohe Anforderungen an Datenherkunft, Nachvollziehbarkeit, Prüfung

Darstellung z.T. aus: Ergebnisbericht DAV zur Validierung v.t. Rückstellungen in der Lebensversicherung unter Solvency II S. 9

DATENQUALITÄT ANFORDERUNGEN
ART 19 DVO

Angemessenheit

Daten
- sind geeignet für Verwendungszweck
- verursachen keine wesentlichen Schätzfehler
- sind im Einklang Annahmen & Techniken
- spiegeln die Risiken angemessen wider
- sind in transparenter, strukturierter Weise in einem dokumentierten Prozess erhoben
- im Zeitverlauf einheitlich verwendet

Vollständigkeit

Daten
- decken alle wichtigen Risikogruppen im Portfolio ab
- verfügen über einen ausreichenden Detaillierungsgrad
- liefern ausreichend historische Informationen

Exaktheit

Daten
- sind ohne **Fehler oder Auslassungen** und Verzerrungen
- Müssen **zeitnah** und **einheitlich** im Zeitablauf sein
- Müssen ein **hohes Maß an Sicherheit** aufweisen
- **Vertrauenswürdigkeit wird durch die Nutzung im Betriebsablauf-** und Entscheidungsprozess nachgewiesen werden.

SCHNITTMENGE AKTUARIELLE PROZESSE ZU IDV
BEISPIEL: VALIDIERUNGSPROZESS RÜCKSTELLUNG

	Validierungsprozess	IDV VAIT	Maßnahme
Governance, Dokumentation	› Validierungshandbuch › Validierungsbericht › „Kontrollberichte“ hinsichtlich IKS	› IDV-Richtlinie › Beschreibung der einzelnen IDV-Anwendung	› Widerspruchsfreie „Leitfäden“ › Verweistechnik reduziert Redundanz, Pflegeaufwand
Risiko-orientierung	› Schwerpunkt auf kritische Bereiche › Proportionalitätsprinzip	› Schwerpunkt auf kritische Prozesse › Proportionalität (VAIT Tz. 6)	› Schnittmenge hinsichtlich Konsistenz überprüfen
Change-management	› Festlegung Umgang Änderungen im Modell/Bewertung/Verfahren	› Änderungen häufig mit IDV-Anpassungen verbunden	› Abstimmung der Freigabeverfahren
Funktions-trennung Fachabteilung	(Grundsätzlich) personelle Trennung der Validierung vom Erstellungs-prozess	Trennung Entwicklung/Test (Technische und fachliche Prüfung)	› Rollenverteilung überprüfen

» „Synergieeffekte" «

» Konsistenz erforderlich «

MAZARS
Roever Broenner Susat Mazars

4.

Praxiserfahrungen

WORAN MANGELT ES HÄUFIG IN DER PRAXIS?
ERFAHRUNG AUS VERGLEICHBAREN THEMEN

- Einbindung der IDV in IT Strategie, IT-Sicherheit und IT- Risikomanagement
- IDV Richtlinie mit verbindlichen Vorgaben für die Fachbereiche
- Erhebung aller IDV, angemessene Feststellung der Wesentlichkeit und des Schutzbedarfs
- Programmierrichtlinien, Benutzerberechtigungsmanagement
- Versionierung und Aufbewahrung von Programm- und Ergebnisversionen
- Test und Freigabe im 4- Augenprinzip, regelmäßiger Formelcheck
- Nachvollziehbare technische Programmdokumentation, Anwenderdokumentation, Tests etc.
- Fehlende Rückkopplung zur IDV-Fachabteilung bei Änderungen in Zuliefersysteme
- Designrisiken:
  - Keine Trennung von Eingabe, Datenhaltung, Berechnung
  - Hohe Anzahl von Tabellen und Verweisen
  - Sehr individuelle Programmierung
- Nachvollziehbarkeit von Datenänderungen

SUMMARY

Wesentliche Handlungsfelder IDV	
1.	**Bestandsaufnahme** IDV von den Fachbereichen, mit Dokumentation und besonderer Berücksichtigung kritischer IDVs und Ermittlung des jeweiligen Schutzbedarfs
2.	**IDV Richtlinie** (Verantwortlichkeiten, Aufgabenverteilung, Standards)
3.	Schaffung und Umsetzung von **Programmierstandards, Qualitätssicherungsverfahren** sowie **Testverfahren im Vier-Augen-Prinzip**
4.	**Versionierung** und unveränderbare **Aufbewahrung** von Programmen und Ergebnissen
5.	Verwendung von **IDV Funktionalitäten innerhalb der Anwendungen**, um das Fehlerrisiko während der betrieblichen Nutzung zu minimieren
6.	Schaffung einer **Programm- und Datenzugriffskontrolle** in Abhängigkeit vom jeweiligen IDV-Risiko
7.	**Nachvollziehbarkeit und Prüfbarkeit:** Verfahrensdokumentation (fachlich, technisch, Anwender) **Nachweise:** Änderungen, Tests, Fehlerhebung, Benutzer- und Berechtigungen etc.
8.	**Qualität von Quelldaten** sowie **Audit-Trail** für Datenänderungen bei der Zulieferung, in den IDV Dateien oder den IDV Ergebnissen

Ihre Fragen?

IHRE ANSPRECHPARTNER

Ralf Engelshove

Wirtschaftsprüfer
Steuerberater
Partner

Mazars GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Gustav-Heinemann-Ufer 72
50968 Köln

Tel: +49 221 28 20 – 25 60
ralf.engelshove@mazars.de

Detlef Lochmann

CISA/ ISACA/ ISMS Lead Auditor
nach ISO 27001
Diplom-Ökonom
Director

Mazars GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Bennigsen-Platz 1
40474 Düsseldorf

Tel: +49 211 83 99 – 620
detlef.lochmann@mazars.de

Mazars GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

www.mazars.de