Besser Barmenia. Besser leben.

Barmenia Versicherungen

Leben | Kranken | Unfall | Sach

Compliance-Erfüllung durch Automatisierung
Mehr Chance als nur Kosten

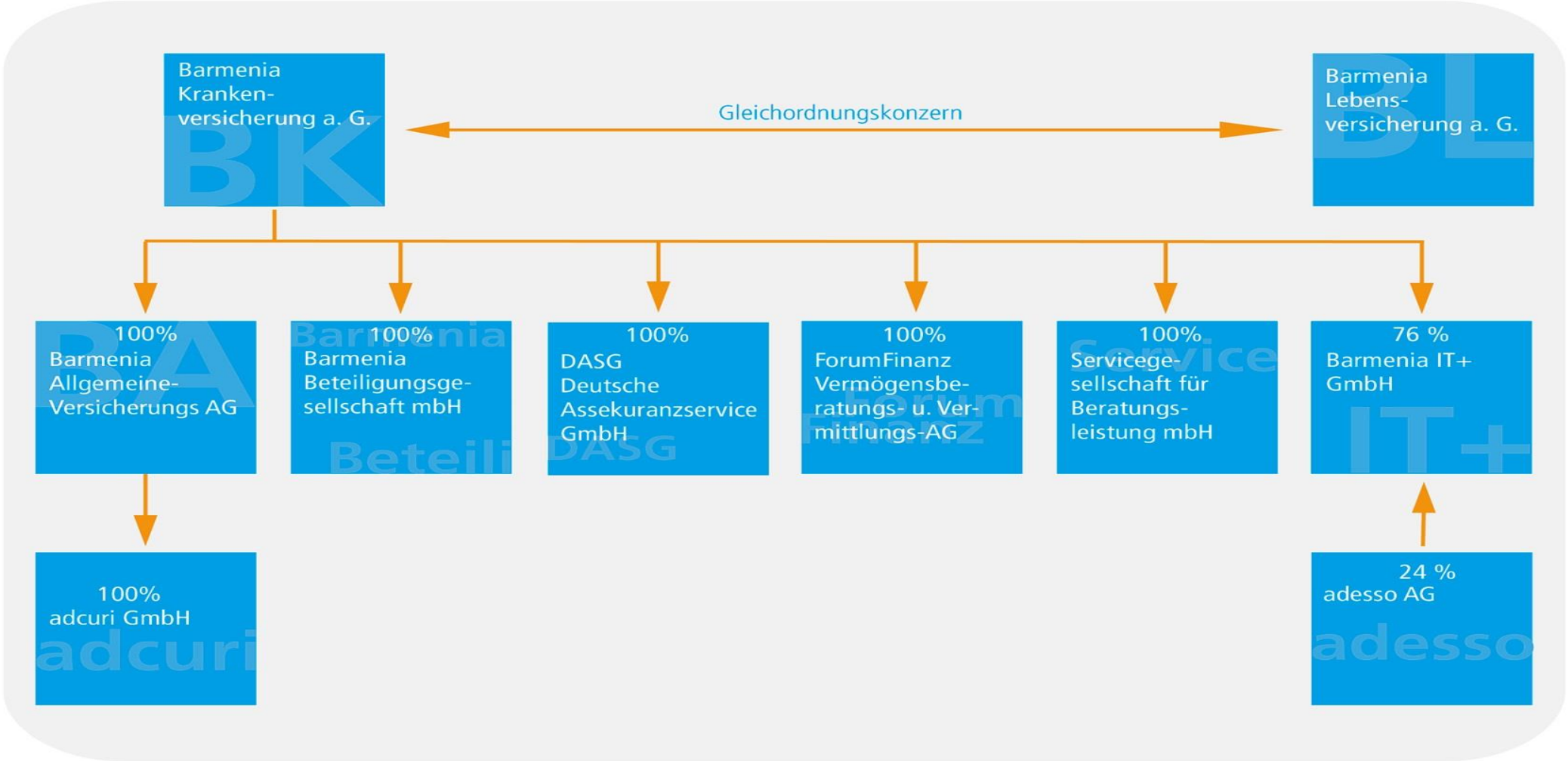
Andre Lünsmann
Barmenia Krankenversicherung a.G.

18.10.2018

Vortragsinfos

- Was bedeutet Compliance zu Zeiten von Digitalisierung (für Versicherungen) und was muss man dafür alles tun?
- Warum spielt die IT-Strategie im Kontext von DSGVO und VAIT eine wichtige Rolle und wie sorgt man für zielgerichtetes Handeln aller Beteiligten?
- Warum ein Cloud Ansatz auch für Compliance Lösungen hilfreich sein kann.
- Wie kann Compliance mehr Chance als nur Kosten sein?

Barmenia Konzern



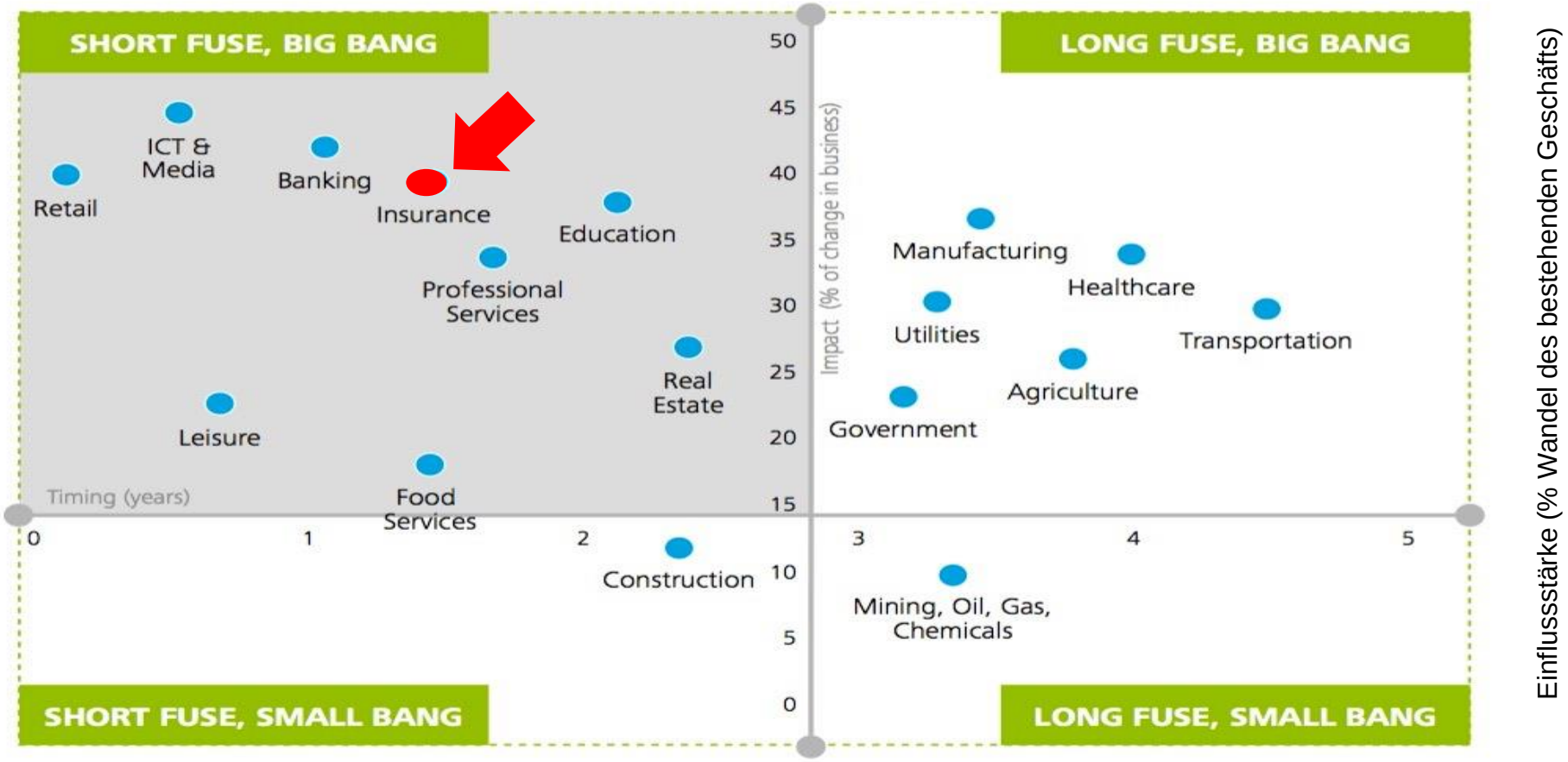
Barmenia Versicherungen

Vortragsinfos

- **Was bedeutet Compliance zu Zeiten von Digitalisierung (für Versicherungen) und was muss man dafür alles tun?**
- Warum spielt die IT-Strategie im Kontext von DSGVO und VAIT eine wichtige Rolle und wie sorgt man für zielgerichtetes Handeln aller Beteiligten?
- Warum ein Cloud Ansatz auch für Compliance Lösungen hilfreich sein kann.
- Wie kann Compliance mehr Chance als nur Kosten sein?

Versicherungen werden stark von Änderungen betroffen sein

Etablierte Branchen werden einen „großen Knall“ erleben – Versicherer sind stark betroffen.



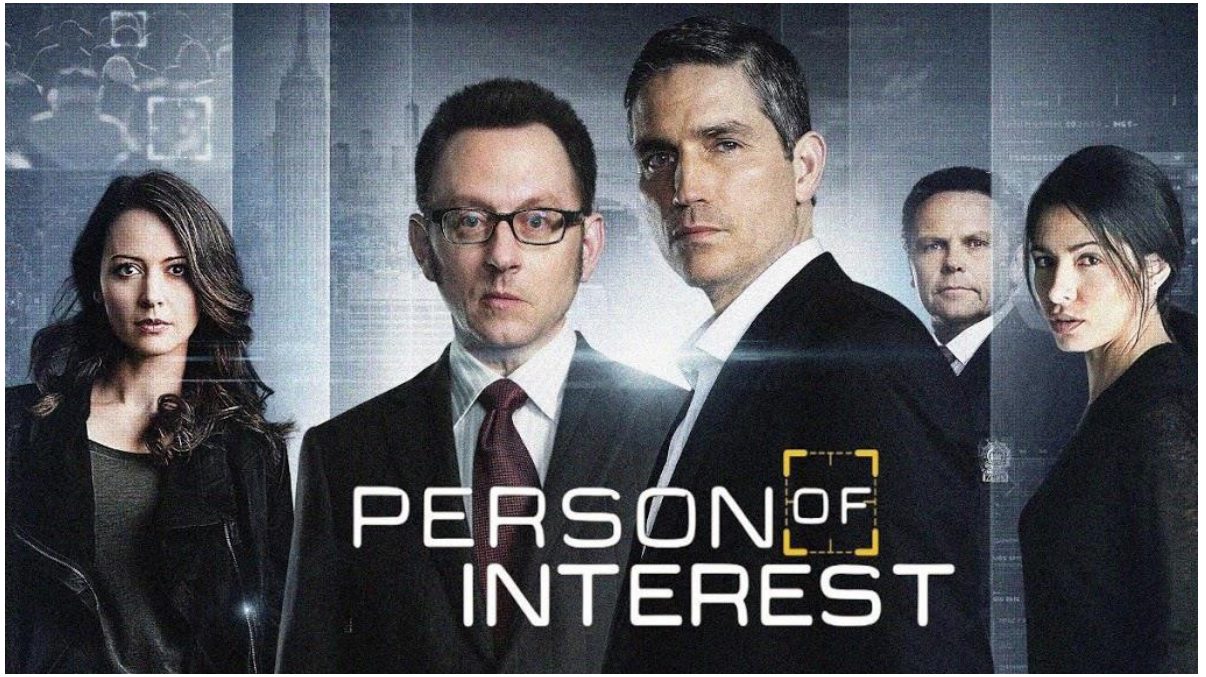
Zeitverlauf (Jahre)

Einflussstärke (% Wandel des bestehenden Geschäfts)

Barmenia Versicherungen

Compliance – Wie es (nicht) sein sollte

Serie von 2011/2012
Der Erfinder einer für den Staat entwickelten Überwachungsmaschine hat Bedenken wegen unschuldiger Opfer aus der Bevölkerung, die dem US Staat egal sind.
Er versucht mit seiner „Maschine“, die „gute“ Seite der von ihm gebauten Maschine zu retten, damit auch Verbrechen an Unschuldigen verhindert werden.
Gejagt wird er und seine Helfer von der Maschine und dem Sicherheitspersonal des US Staates.
Es werden viele technische Raffinessen gezeigt, die aber heute alle möglich sind!

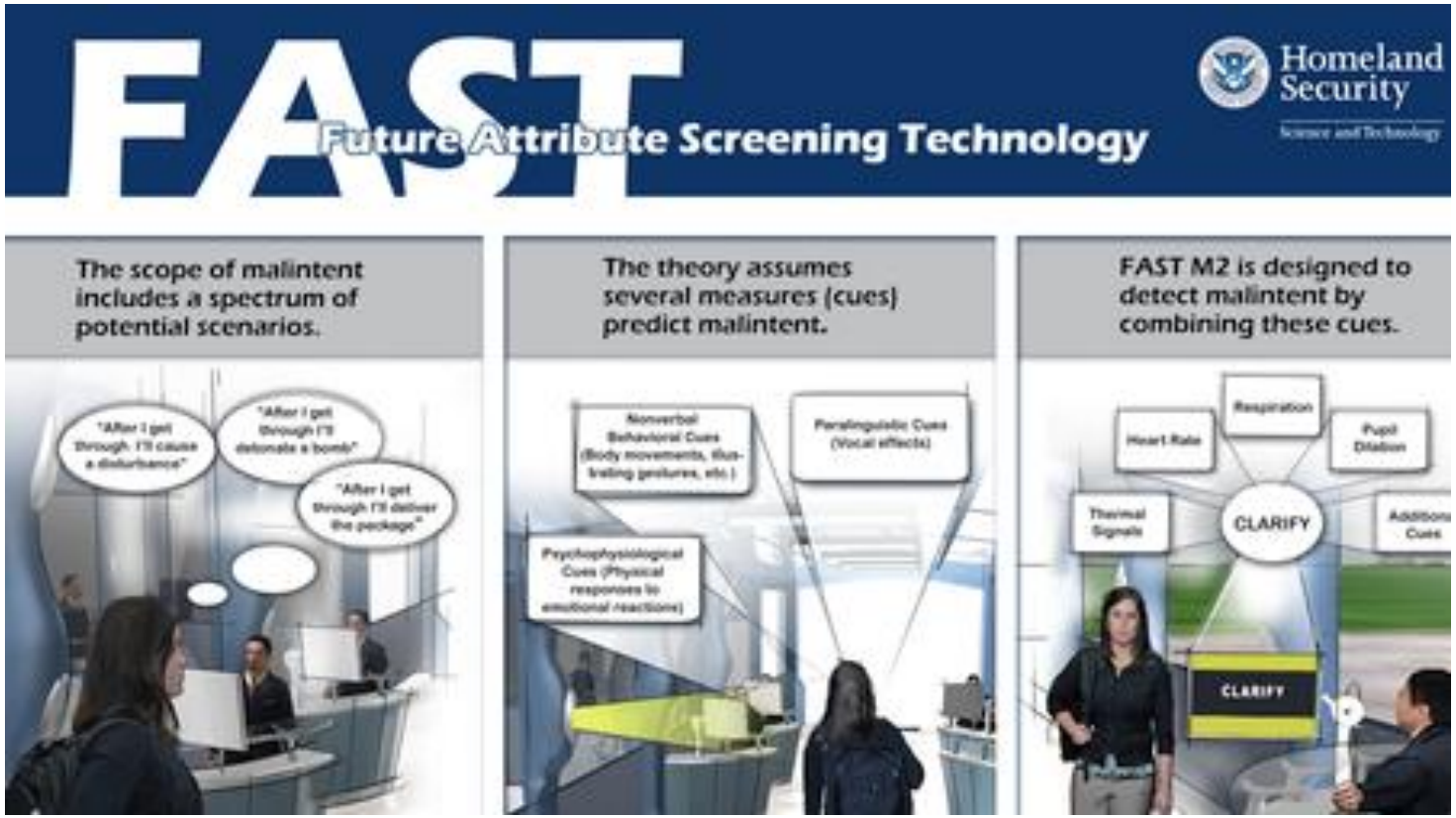


Barmenia Versicherungen

Compliance – Wie es (nicht) sein sollte

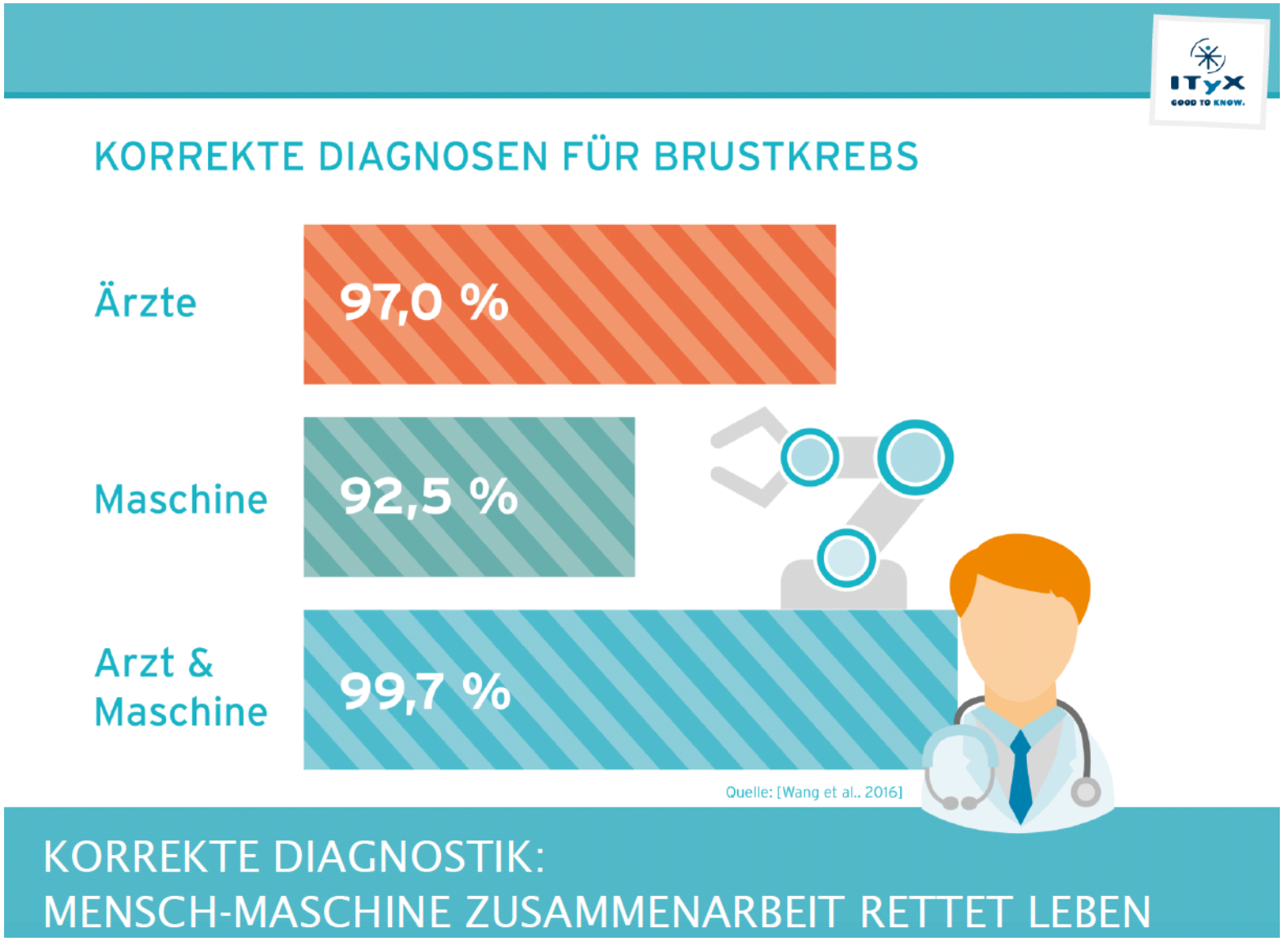
Homeland Security

FAST steht für
Future Attribute Screening Technology
Ein Testlauf zeigte eine Erfolgsrate von 78%



Barmenia Versicherungen

Wenn künstliche Intelligenz dem Arzt bei Diagnosen hilft



Quelle: Andreas Klug Vorsitzender AI Verbund bitkom

Barmenia Versicherungen

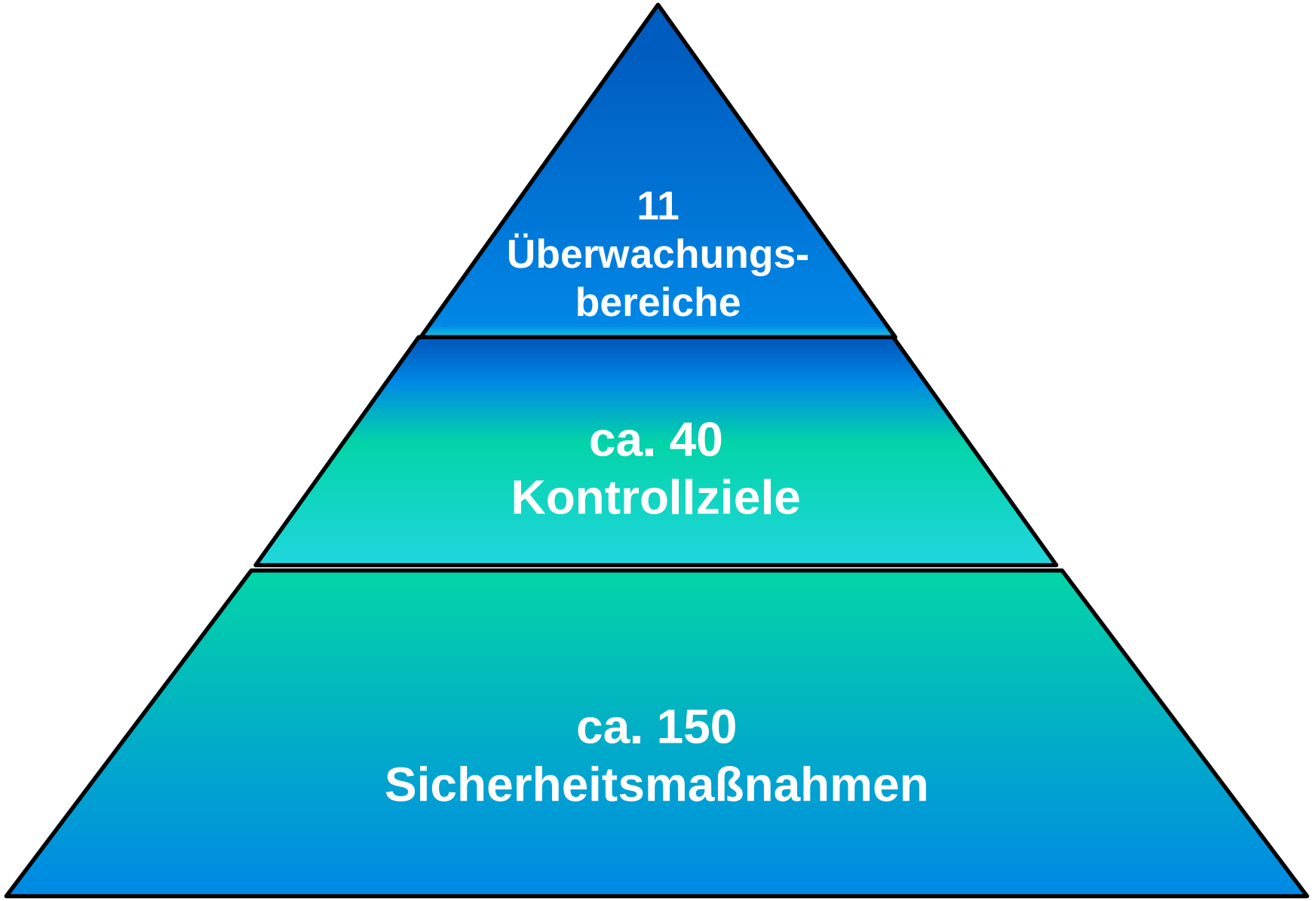
Gesetzgebungen und ISO

- Mindestanforderungen an das Risikomanagement (MaRisk) -2010-
- ~~Bundesdatenschutzgesetz alte Fassung (BDSG) -1990-~~
- ~~Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) -2014-~~
- International Organization for Standardization (ISO 27002) -2014-
- Bundesdatenschutzgesetz neue Fassung (BDSG) -2017-
- EU-Datenschutz-Grundverordnung (DSGVO) -2018-
- Versicherungsaufsichtliche Anforderungen an die IT (VAIT) -2018-

MaRisk

- Gilt im Finanzdienstleistungssektor
- Bei der Ausgestaltung der IT-Systeme und IT-Prozesse sind grundsätzlich gängige Standards einzuhalten. Zu den Standards gehören u.a.
  - Inhalte des IT-Grundschutzhandbuchs des BSI
  - Standards sind ISO 2700x etc.
- Die Daten, Methoden und Verfahren müssen dokumentiert und die Wirksamkeit regelmäßig geprüft und sichergestellt werden.
- Die Programmtechnische Freigabe erfolgt unabhängig vom Anwender.
- Produktions- und Testumgebungen sind zu trennen.

Inhalte aus ISO 27001/27002 usw.



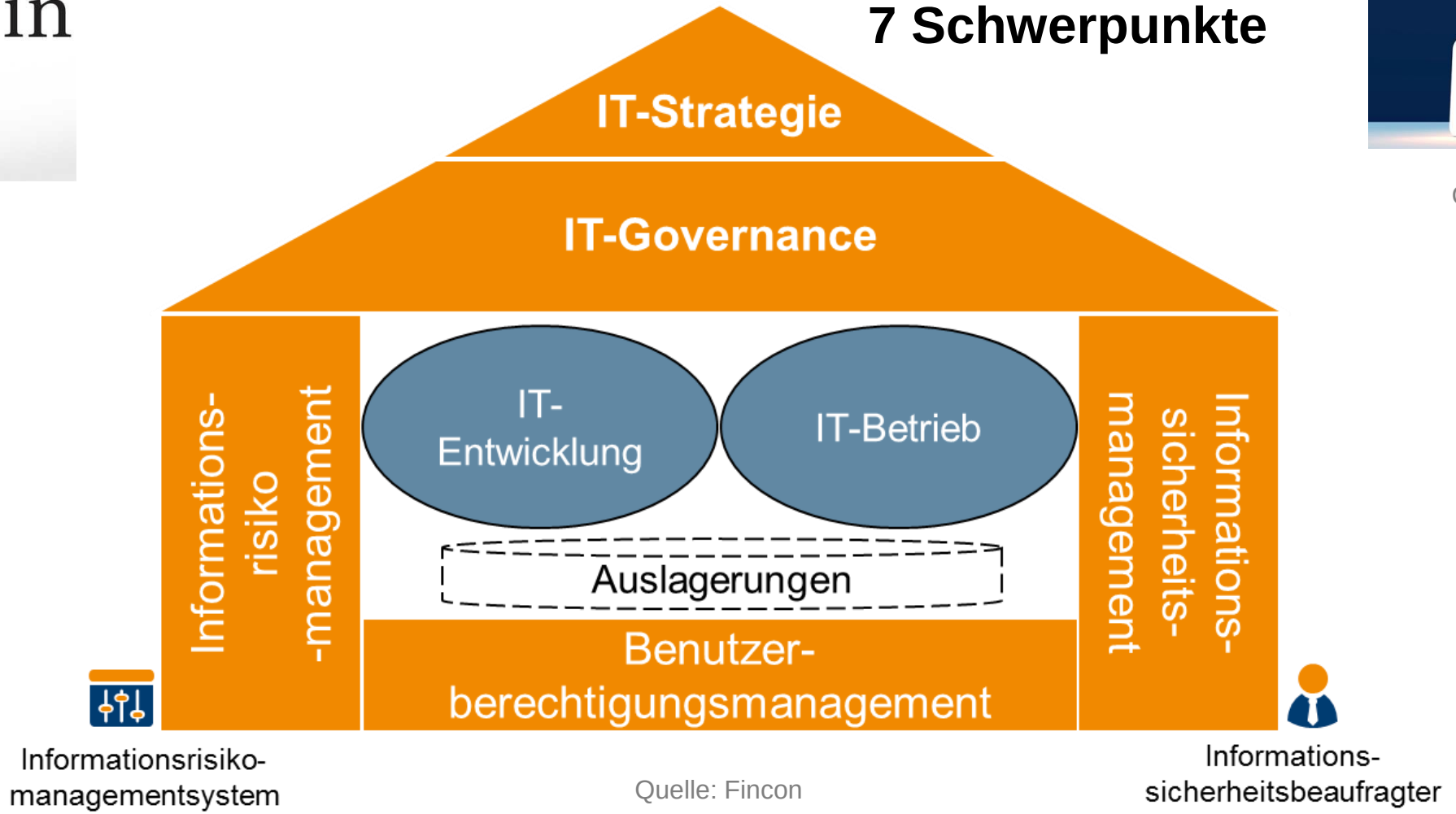
Barmenia Versicherungen

Versicherungsaufsichtliche Anforderungen an die IT (VAIT)

BaFin

7 Schwerpunkte

Quelle: BaFin



Quelle: Fincon

Barmenia Versicherungen

Juristische Quelle

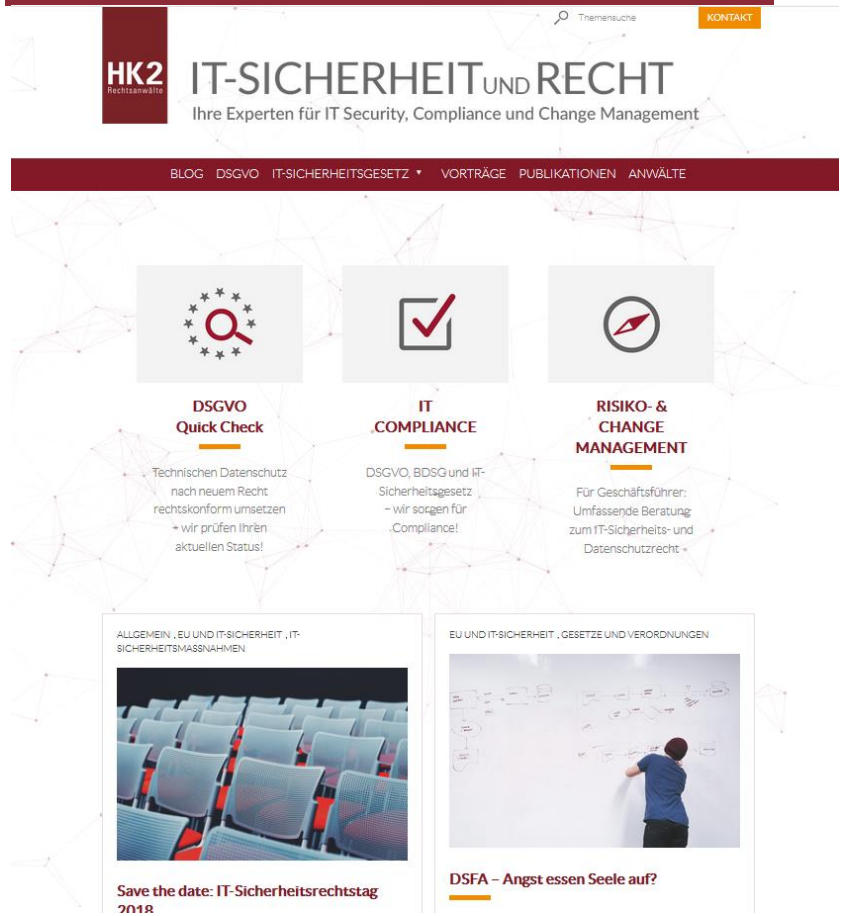
Karsten U. Bartels LL.M.*

- Partner/ Rechtsanwalt, HK2 Rechtsanwälte
- Geschäftsführer HK2 Comtection GmbH
- Zert. Datenschutzbeauftragter (TÜV)
- Vorstand Bundesverband IT-Sicherheit e. V. (TeleTrusT)
- Stellv. Vorsitzender Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e. V.

*Rechtsinformatik

Juristische Quelle

www.it-sicherheit-und-recht.de



HK2 – Der Rote Faden

Count-up: 27 Tage DSGVO

Updates, Tipps und To Do's rund um die Datenschutzgrundverordnung

WhatsApp, Slack und Co. in der betrieblichen Kommunikation...

Im Rahmen der Vorbereitung auf die DSGVO wurden in zahlreichen Unternehmen die datenschutzrechtlichen Prozesse auf den Prüfstand gestellt.

Eine Frage, die dabei erstaunlich oft aufkam: „Darf ich **WhatsApp** (oder andere Messenger-Dienste) auf dem **Diensthandy** bzw. dienstlich genutzten Privathandy nutzen? ". Die **kurze Antwort** lautet **„Nein!"**. Bei Installation wird nämlich das gesamte **Adressbuch ausgelesen**, wobei die **Daten** auf **Servern** in den **USA** landen.

DSFA - Angst essen Seele auf?

Die DSGVO sieht in Art. 35 vor, dass bei einer Datenverarbeitung mit **hohem Risiko** für „Rechte und Freiheiten natürlicher Personen" eine sog. **Datenschutzfolgenabschätzung** (DSFA) durchzuführen ist.

Folglich ist bei **bestimmten Verarbeitungsvorgängen** von **personenbezogenen Daten abzuschätzen**, welche **Folgen** sie für den Schutz dieser Daten haben. Wann dies der Fall ist, wird sehr allgemein und nicht abschließend in Art. 35 Abs. 3 DSGVO dargestellt. Eine Hilfestellung zur Risikobewertung fehlt.

www.hk2.eu/newsletter

Folgen von Verstößen

Folgen von Verstößen
Art. 83 Abs. 4, 5 DSGVO

Bußgelder bis EUR 10.000.000 bzw. EUR 20.000.000 oder 2 % bzw. 4 % des weltweiten Vorjahresumsatzes

Auslagerung

Wer hat seine IT per Outsourcing verlagert?

Ist Compliane dann für Sie noch ein Thema oder macht das primär der Anbieter?

Barmenia Versicherungen

Auslagerung

Art. 32 Versicherungsaufsichtsgesetz (VAG)

(1) Ein Versicherungsunternehmen, das Funktionen oder Versicherungstätigkeiten ausgliedert, bleibt für die Erfüllung aller aufsichtsrechtlichen Vorschriften und Anforderungen verantwortlich.

(2) Durch die Ausgliederung dürfen die ordnungsgemäße Ausführung der ausgegliederten Funktionen und Versicherungstätigkeiten, die Steuerungs- und Kontrollmöglichkeiten des Vorstands sowie die Prüfungs- und Kontrollrechte der Aufsicht[…]s ausgliedernde Unternehmen hinsichtlich der von der Au[…]keiten sicherzustellen, dass

1. das Unternehmen selbs[…]aten zugreifen können,
2. der Dienstleister mit der[…]
3. die Aufsichtsbehörde Zu[…]ie selbst oder durch Dritte ausüben kann.

(3) Bei der Ausgliederung wic[…]cherungsunternehmen außerdem sicherzustellen, dass wese[…]isation, eine übermäßige Steigerung des operationel[…] zufriedenstellenden Dienstleistung für die Versi[…]

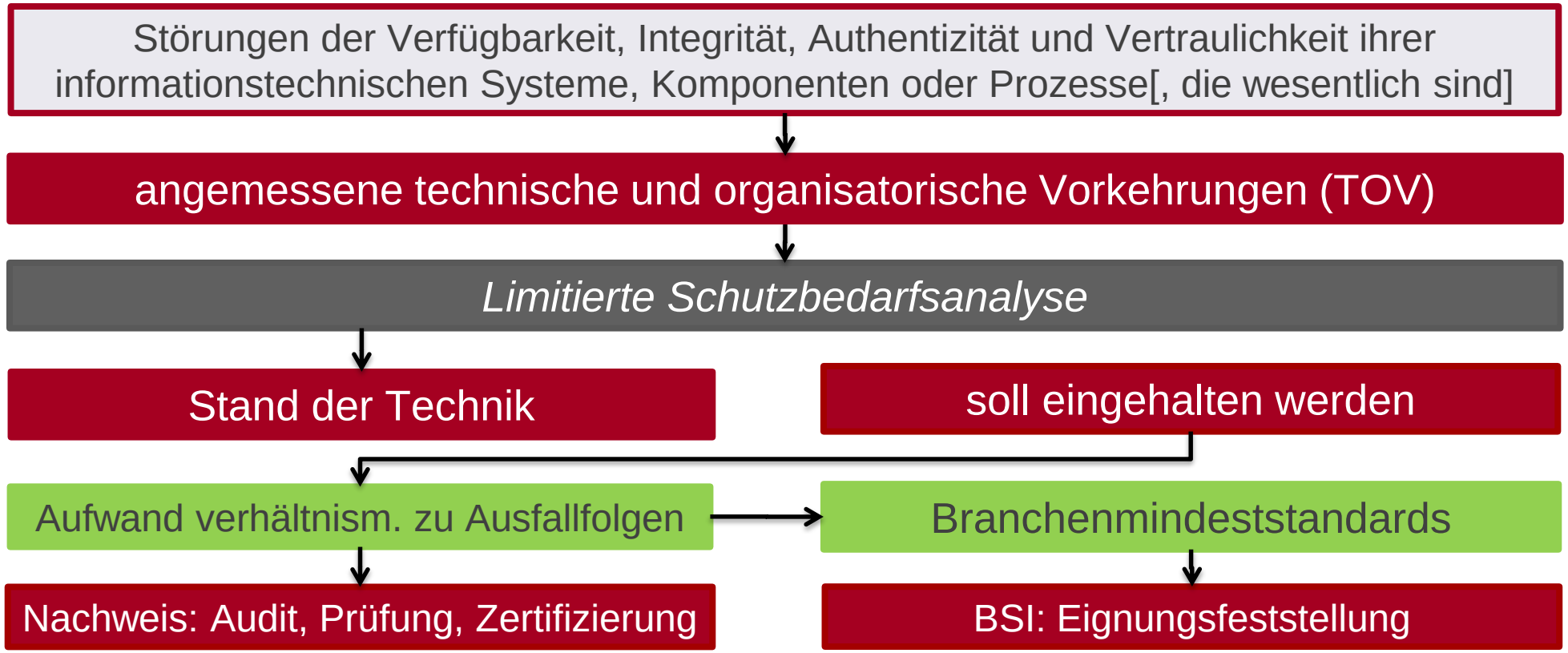
(4) Das ausgliedernde Versicherungsunternehmen hat sich die erforderlichen Auskunfts- und Weisungsrechte vertraglich zu sichern und die ausgegliederten Funktionen und Versicherungstätigkeiten in sein Risikomanagement einzubeziehen. Ein Weisungsrecht ist dann nicht erforderlich, wenn im Rahmen einer steuerlichen Organschaft Funktionen auf eine Muttergesellschaft ausgegliedert werden und diese sich für die Wahrnehmung der Funktionen oder Versicherungstätigkeiten vertraglich den gleichen aufsichtsrechtlichen Anforderungen unterwirft, die für das ausgliedernde Unternehmen gelten.

Irrglaube!
„Mit Outsourcing bin ich raus aus der Thematik!“

HK2 Rechtsanwälte

Barmenia Versicherungen

Betreiber kritischer Infrastrukturen sind verpflichtet, zur Vermeidung von (§ 8a BSIG)



Stand der Technik ist…

…der Entwicklungsstand **fortschrittlicher** Verfahren, Einrichtungen oder Betriebsweisen, der die **praktische Eignung** einer Maßnahme zum Schutz der Funktionsfähigkeit der informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der **Verfügbarkeit, Integrität, Authentizität** und **Vertraulichkeit gesichert erscheinen lässt**.

[Gesetzesbegründung zu § 8a BSIG, BT-Drucks. 18/4096, S. 26]

Quelle: Karsten Bartels HK2

Beim Stand der Technik handelt es sich um

…die im Waren- und Dienstleistungsverkehr **verfügbaren** Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele **am wirkungsvollsten** gewährleisten kann.

Bartels/ Backer/ Schramm: Der „Stand der Technik“ im IT-Sicherheitsrecht – Wirkung des Verweisungsbegriffs und Lösungsansätze zur legislativen Verwendung, Tagungsband 15. Deutscher IT-Sicherheitskongress 2017, S. 503

Quelle: Karsten Bartels HK2

Stand der Te

Handreichung zum Stand der Technik

Bundesverband IT-Sicherheit e. V.

68 Seiten detaillierte Infos

Infoveranstaltung in Berlin am 25.10.2018

https://www.teletrust.de/veranstaltungen/it-sicherheitsgesetz-und-dsgvo/it-sicherheitsrechtstag-2018/

1.1 IT-Sicherheitsgesetz ... 7
1.2 Branchenspezifische Sicherheitsstandards des BSI für KRITIS-Betreiber ... 8
1.3 Europäische Implikationen ... 9
1.4 Datenschutz-Grundverordnung ... 9
1.5 Angemessenheit der Maßnahmen ... 10

2 Bestimmung des Technologiestandes ... 11
2.1 Begriffsklärung ... 11
2.2 Methode zur Bestimmung des Technologiestandes ... 12
2.3 Prozess zur Qualitätssicherung der Handreichung ... 13
2.4 Geforderte Schutzziele ... 14

3 Technische und organisatorische Maßnahmen (TOMs) ... 15
3.1 Allgemeine Hinweise ... 15
3.2 Technische Maßnahmen ... 17
3.2.1 Bewertung der Passwortstärke ... 17
3.2.2 Durchsetzung starker Passwörter ... 19
3.2.3 Multifaktor-Authentifizierung ... 21
3.2.4 Kryptographische Verfahren ... 23
3.2.5 Verschlüsselung von Festplatten ... 25
3.2.6 Verschlüsselung von Dateien und Ordnern ... 26
3.2.7 Verschlüsselung von E-Mails ... 28
3.2.8 Sicherung des elektronischen Datenverkehrs mit PKI ... 29
3.2.9 Einsatz von VPN (Layer 3) ... 32
3.2.10 Verschlüsselung auf Layer 2 ... 35
3.2.11 Cloudbasierter Datenaustausch ... 36
3.2.12 Datenablage in der Cloud ... 37
3.2.13 Nutzung von mobilen Sprach- und Datendiensten ... 39
3.2.14 Kommunikation mittels Instant-Messenger ... 40
3.2.15 Management mobiler Geräte ... 42
3.2.16 Routersicherheit ... 43
3.2.17 Netzwerküberwachung mittels Intrusion Detection System ... 45
3.2.18 Schutz des Web-Datenverkehrs ... 47
3.2.19 Schutz von Webanwendungen ... 48
3.2.20 Fernzugriff auf Netzwerke / Fernwartung ... 50
3.3 Organisatorische Maßnahmen ... 51
3.3.1 Standards und Normen ... 52
3.3.2 Prozesse ... 55
3.3.2.1 Sicherheitsorganisation ... 56
3.3.2.2 Anforderungsmanagement ... 57
3.3.2.3 Management des Geltungsbereichs ... 58
3.3.2.4 Management der Informationssicherheits-Leitlinie ... 59
3.3.2.5 Risikomanagement ... 59
3.3.2.6 Management der Erklärung zur Anwendbarkeit ... 59
3.3.2.7 Ressourcenmanagement ... 59
3.3.2.8 Wissens- und Kompetenzmanagement ... 60
3.3.2.9 Dokumentations- und Kommunikationsmanagement ... 60
3.3.2.10 IT-Servicemanagement ... 60
3.3.2.11 Management der Erfolgskontrolle ... 62
3.3.2.12 Verbesserungsmanagement (kontinuierlicher Verbesserungsprozess) ... 63
3.3.3 Sichere Softwareentwicklung ... 63
3.3.4 Audits und Zertifizierung ... 65

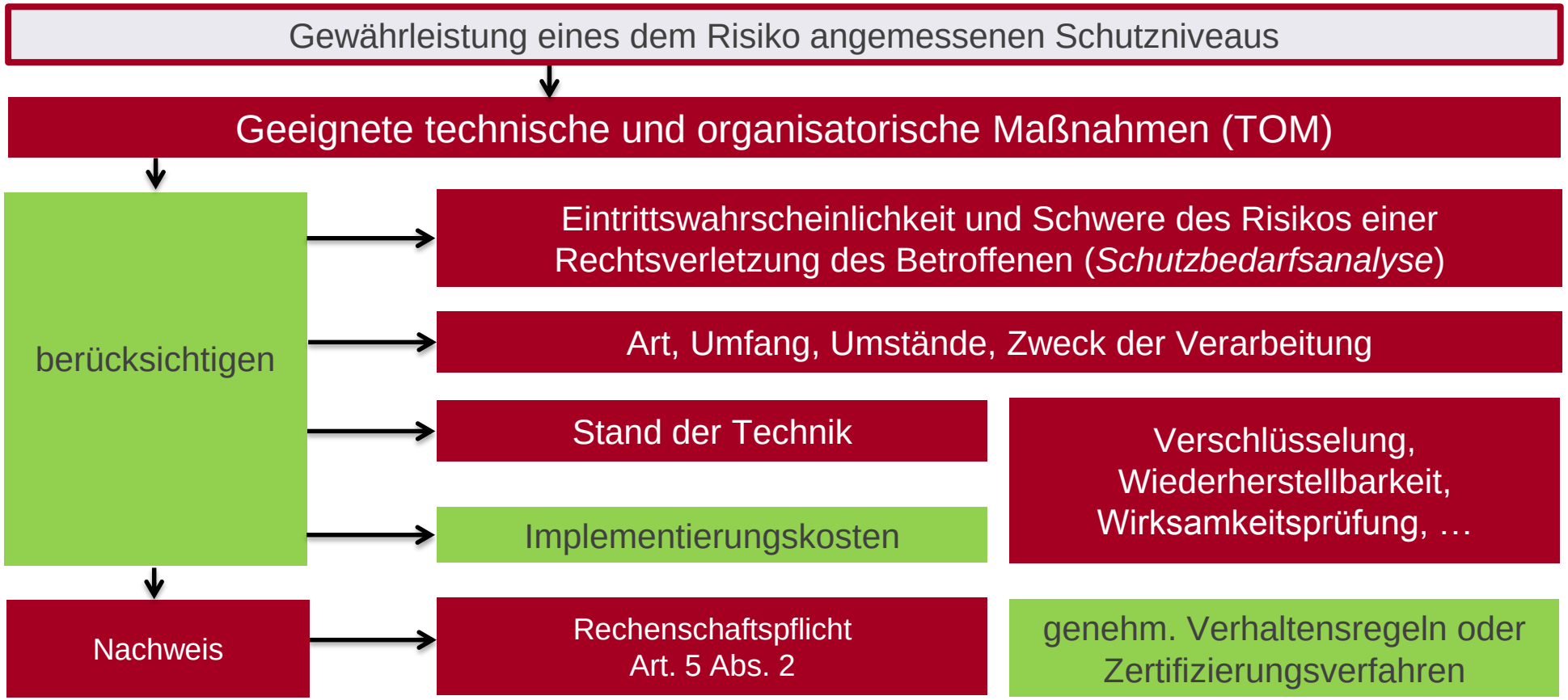
Quelle: Karsten Bartels HK2

Grundsätze und Verantwortlichkeit (Art. 5 DSGVO)

1) Personenbezogenen Daten müssen…
   … Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz
   … Zweckbindung
   … Datenminimierung
   … Richtigkeit
   … Speicherbegrenzung
   … **geeignete technische und organisatorischen Maßnahmen** (Integrität und Vertraulichkeit)
2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen **Einhaltung nachweisen können** (**Rechenschaftspflicht**)

Quelle: Karsten Bartels HK2

Art. 32 DSGVO: Sicherheit der Verarbeitung



Datenschutz – Folgeabschätzung (DSFA) Art. 35 DSGVO

Voranalyse

- Bei **vorrausichtlich hohem Risiko** der Verarbeitung (Prognose), insbesondere,
  - bei Verwendung neuer Technologien
  - nach Art, Umfang, Umstände und Zwecke der Verarbeitung
- Immer bei
  - systematischer u. umfassender Bewertung persönlicher Aspekte natürlicher Personen
  - Verarbeitung bes. Kategorien v. personenbezogenen Daten
  - Überwachung öffentlich zugänglicher Bereiche
  - Ausdrückliche Bestimmung durch Aufsichtsbehörde
- Nie bei
  - Ausdrückliche Bestimmung durch Aufsichtsbehörde

Datenschutz-Folgenabschätzung

- Systematische Beschreibung der Verarbeitungsvorgänge und Zwecke
- Bewertung von Notwendigkeit und Verhältnismäßigkeit
- Bewertung der Risiken
- Geplante Abhilfemaßnahmen
- …

Hohes Risiko

Normales Risiko

Konsultation der Aufsichtsbehörde

Verarbeitung

Empfehlung/ Untersuchung/ Abhilfe

HK2 Rechtsanwälte

Barmenia Versicherungen

Konkretisierungen nach VAIT

Umsetzung der IT-Strategie durch die Geschäftsleitung

- Strategische Entwicklung der IT-Architektur.
- Darstellung des Zielbilds der IT-Architektur.
- Die in der IT-Strategie niedergelegten Ziele sind so zu formulieren, dass eine sinnvolle Überprüfung der Zielerreichung möglich ist.
- Die IT-Strategie ist bei Erstverabschiedung sowie bei Anpassungen dem Aufsichtsorgan des Unternehmens zur Kenntnis zu geben und ggf. mit diesem zu erörtern.

Konkretisierungen nach VAIT

IT-Governance

- Die Eignung der IT-Systeme und der zugehörigen IT-Prozesse, die Schutzziele zu erreichen, ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen.
- **Ein angemessenes Verfahren für die Klassifizierung / Kategorisierung (Schutzbedarfsklasse)** und den Umgang mit den von Endbenutzern des Fachbereichs entwickelten oder betriebenen Anwendungen **ist festzulegen**.

Zentrales Register – CMDB –

Für einen Überblick und zur Vermeidung von Redundanzen wird ein zentrales Register der kritischen bzw. wesentlichen Anwendungen geführt. Das Register beinhaltet grundsätzlich zumindest die Anwendungen, die zur Identifizierung, Bewertung, Überwachung und Steuerung der Risiken sowie zur Berichterstattung über diese Risiken eingesetzt werden oder die für die Durchführung anderer versicherungstypischer Tätigkeiten von Bedeutung sind.

Es werden mindestens folgende Informationen erhoben:

- Name und Zweck der Anwendung,
- Versionierung, Datumsangabe,
- Fremd- oder Eigenentwicklung,
- Fachverantwortliche(r) Mitarbeiter,
- Technisch verantwortliche(r) Mitarbeiter,
- Technologie,
- Ergebnis der Risikoklassifizierung/ Schutzbedarfseinstufung und ggf. die daraus abgeleiteten Schutzmaßnahmen.

Berechtigungen

- Berechtigungskonzepte haben des Weiteren die Funktionstrennung zu wahren und Interessenskonflikte des Personals zu vermeiden. Bei IT-gestützter Bearbeitung ist die Funktionstrennung durch entsprechende Verfahren und Schutzmaßnahmen sicherzustellen.
- **Nicht personalisierte Berechtigungen müssen jederzeit zweifelsfrei einer handelnden natürlichen Person (möglichst automatisiert) zuzuordnen sein.** Abweichungen in begründeten Ausnahmefällen und die hieraus resultierenden Risiken sind zu genehmigen und zu dokumentieren.
- **Jeder technische Benutzer muss einer verantwortlichen natürlichen Person zugeordnet sein.**
- **Wesentliche Berechtigungen sind mindestens jährlich zu überprüfen, alle anderen mindestens alle drei Jahre.**

Konkretisierungen nach VAIT

Technisch-organisatorische Maßnahmen sind:

- Auswahl angemessener Authentifizierungsverfahren,
- Implementierung einer Richtlinie zur Wahl sicherer Passwörter,
- automatischer passwortgesicherter Bildschirmschoner,
- **Verschlüsselung von Daten**,
- eine manipulationssichere Implementierung der Protokollierung,
- Maßnahmen zur Sensibilisierung der Mitarbeiter.

Trennung von unvereinbaren Tätigkeiten (VAIT)

- Bei der Ausgestaltung der IT-Aufbau- und IT-Ablauforganisation ist **sicherzustellen, dass miteinander unvereinbare Tätigkeiten durch unterschiedliche Mitarbeiter durchgeführt werden.**

- Interessenkonflikten zwischen Aktivitäten, die beispielsweise im Zusammenhang mit der Anwendungsentwicklung und den Aufgaben des IT-Betriebs stehen, kann durch aufbau- oder ablauforganisatorische Maßnahmen, bspw. durch eine adäquate Rollendefinition, begegnet werden.

Datenschutz, Data Owner (VAIT)

- **Zu den maßgeblichen Stellen gehören auch die Fachbereiche, die Eigentümer der Informationen sind.**
- Die Methodik zur Ermittlung des Schutzbedarfs von Informationen (insbesondere im Hinblick auf die Schutzziele „Integrität“, „Verfügbarkeit“, „Vertraulichkeit“ und "Authentizität") hat die Konsistenz der resultierenden Schutzbedarfe nachvollziehbar sicherzustellen.
  - Schutzbedarfskategorien sind beispielhaft „Niedrig“, „Mittel“, „Hoch“ und „Sehr hoch“.
- Im Rahmen der Anwendungsentwicklung sind nach Maßgabe des Schutzbedarfs angemessene Vorkehrungen im Hinblick darauf zu treffen, dass nach Produktivsetzung der Anwendung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der zu verarbeitenden Daten nachvollziehbar sichergestellt werden.

Revisionssichere Entwicklungsprozesse

- Im Rahmen der Anwendungsentwicklung müssen Vorkehrungen getroffen werden, die erkennen lassen, ob eine Anwendung versehentlich geändert oder absichtlich manipuliert wurde.
- **Sowohl die von Dritten für das Unternehmen entwickelte** als auch die im Unternehmen selbst entwickelte Anwendung ist übersichtlich und für sachkundige Dritte nachvollziehbar zu dokumentieren.
  - Die Dokumentation der Anwendung und ihrer Entwicklung muss zumindest folgende Fragen klären:
    - Was soll entwickelt werden?
    - Wie wurde die Anwendung sowohl technisch als auch prozessual entwickelt?
    - Wie muss die Anwendung betrieben und eingesetzt werden?
  - Zur Nachvollziehbarkeit der Anwendungsentwicklung trägt beispielsweise eine Versionierung des Quellcodes und der Anforderungsdokumente bei.

Timeout !

Barmenia Versicherungen

Vortragsinfos

- Was bedeutet Compliance zu Zeiten von Digitalisierung (für Versicherungen) und was muss man dafür alles tun?
- **Warum spielt die IT-Strategie im Kontext von DSGVO und VAIT eine wichtige Rolle und wie sorgt man für zielgerichtetes Handeln aller Beteiligten?**
- Warum ein Cloud Ansatz auch für Compliance Lösungen hilfreich sein kann.
- Wie kann Compliance mehr Chance als nur Kosten sein?

Warum spielt die IT-Strategie im Kontext von DSGVO und VAIT eine wichtige Rolle und wie sorgt man für zielgerichtetes Handeln aller Beteiligten?

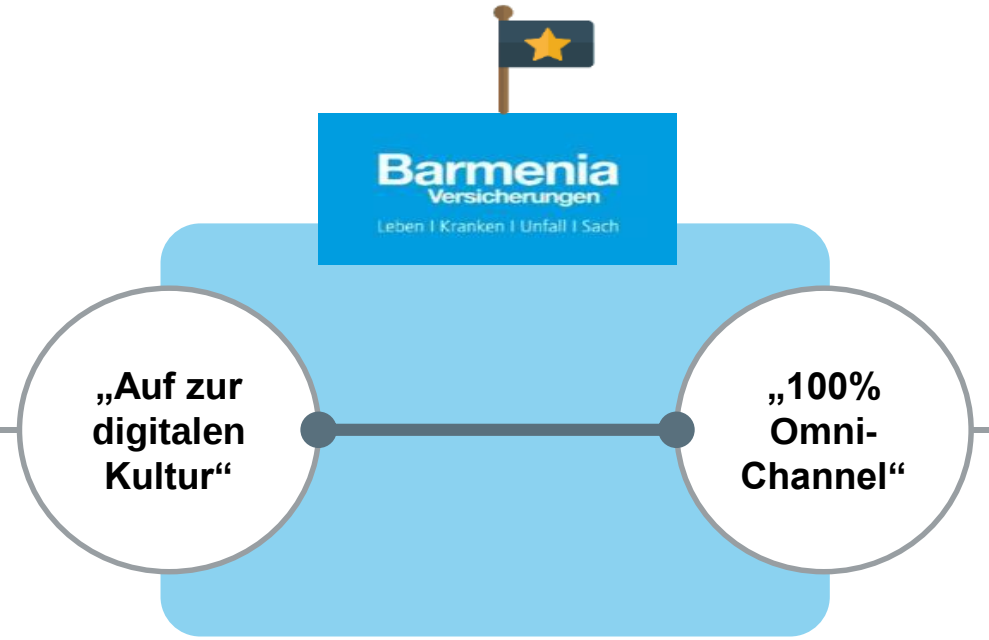
- DSGVO und VAIT verlangen eine Strategie, die auch bis auf die Ebene der ausführenden Mitarbeiter transparent ist.
- Es muss ein IT-Zielbild (Vision) geben.
- Es sollen Standards genutzt werden.
- Prozesse und Verfahren müssen beschrieben und transparent sein.
- Die Einhaltung aller Vorgaben muss kontrolliert werden.
  - Die Kontrollen müssen dokumentiert sein (IKS).
- Es muss zentrale Speichersysteme mit allen Informationen der Systeme geben (CMDB).

IT-Strategie und Ziele

Wir verfolgen zwei strategische Maximen bei der Digitalisierung:
Diese steuern in Form von neun konkreten Leitsätzen unser Handeln.

Kulturelle / verhaltens-orientierte Leitsätze

- Digitalisierung betrifft Alle
- Simply First
- Fertig ist nie
- Big Data – Wissen für Entscheidung



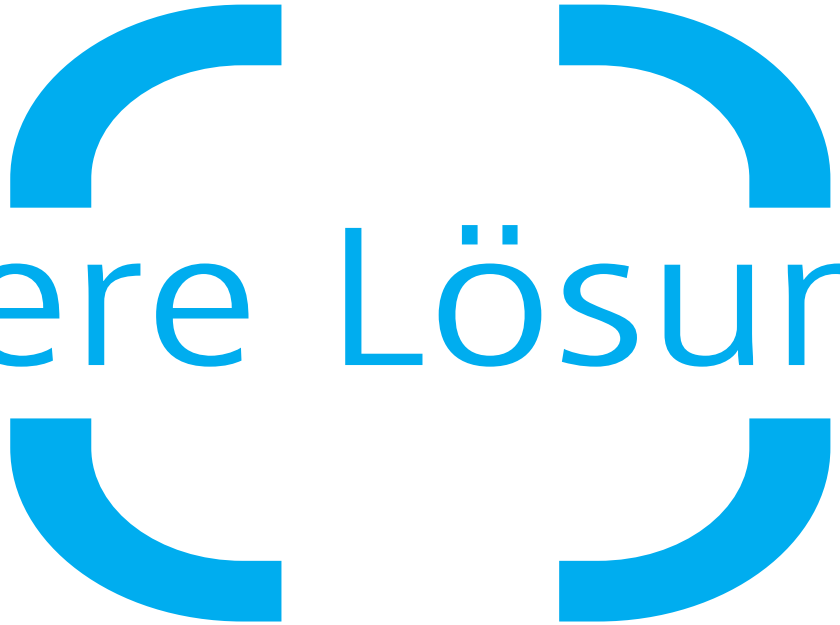
2 strategische Maximen der Digitalisierung des Barmenia-Konzerns

Themenbasierte Leitsätze

- 360° Kundensicht
- Freie Kanalwahl für Alle
- Mobile First
- Max. Self-Service
- Next Best Action

IT-Strategie und Ziele – unsere Vision –

Um die Strategie vermittelbar zu machen, haben wir eine Vision entwickelt.

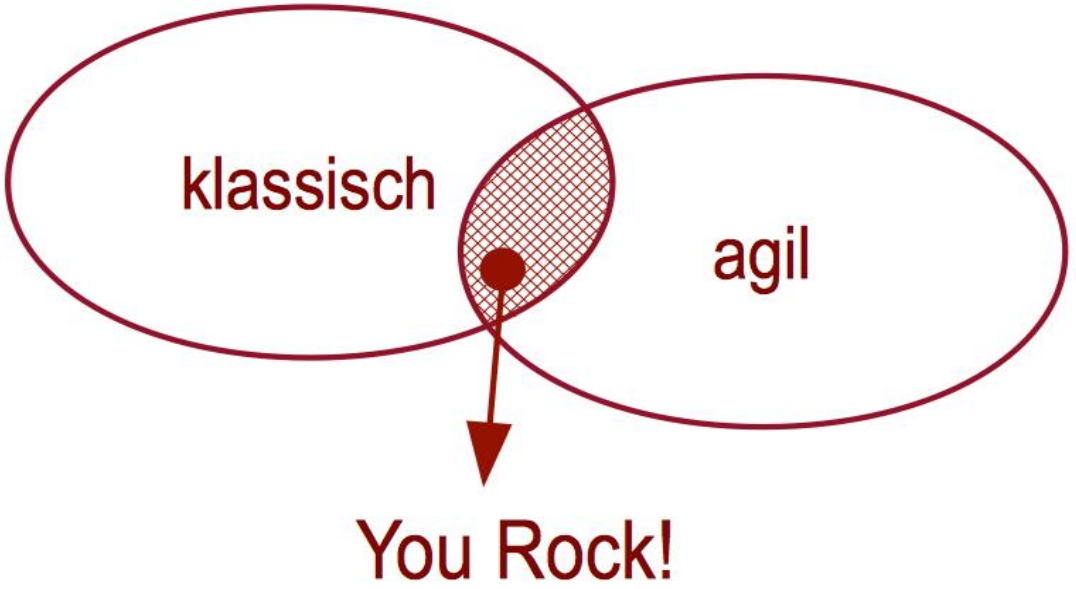


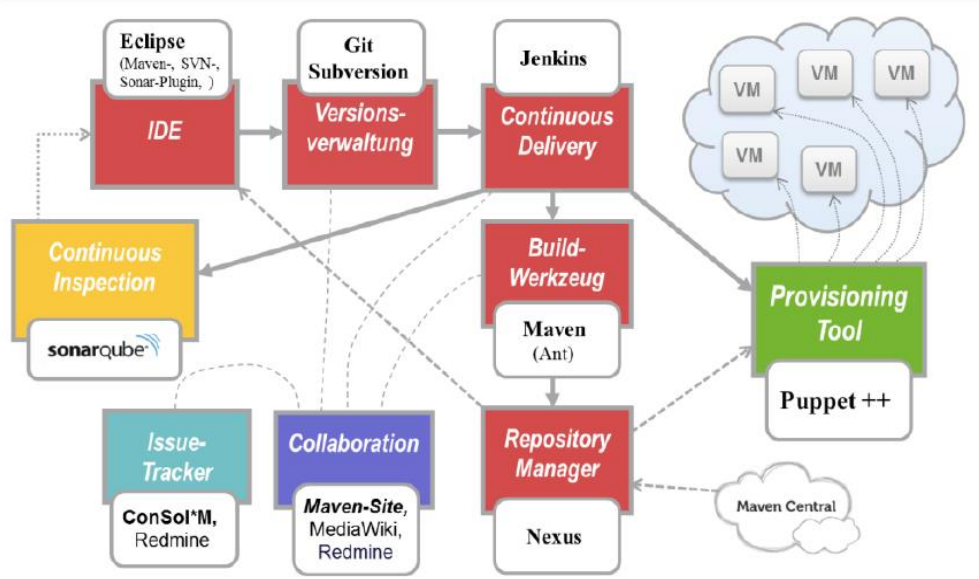
Das bedeutet, unsere Produkte, Prozesse und Strukturen
immer wieder einfacher, schneller und intelligenter
zu machen.

Barmenia Versicherungen

Agilität, DevOps, Standards & Automation, Transparenz

- Zentrales Projektmanagement, gesteuert vom Projekt Office
- Umfassendes Schulungsangebot (CampusLab) für die Mitarbeiter
- Kurze Releasezyklen (< 6 Monate)
- Timeboxing (Verbindlichkeit von Terminen)
- Aufbau von DevOps Teams mit Produktionsverantwortung
- Standardisierung & Automatisierung

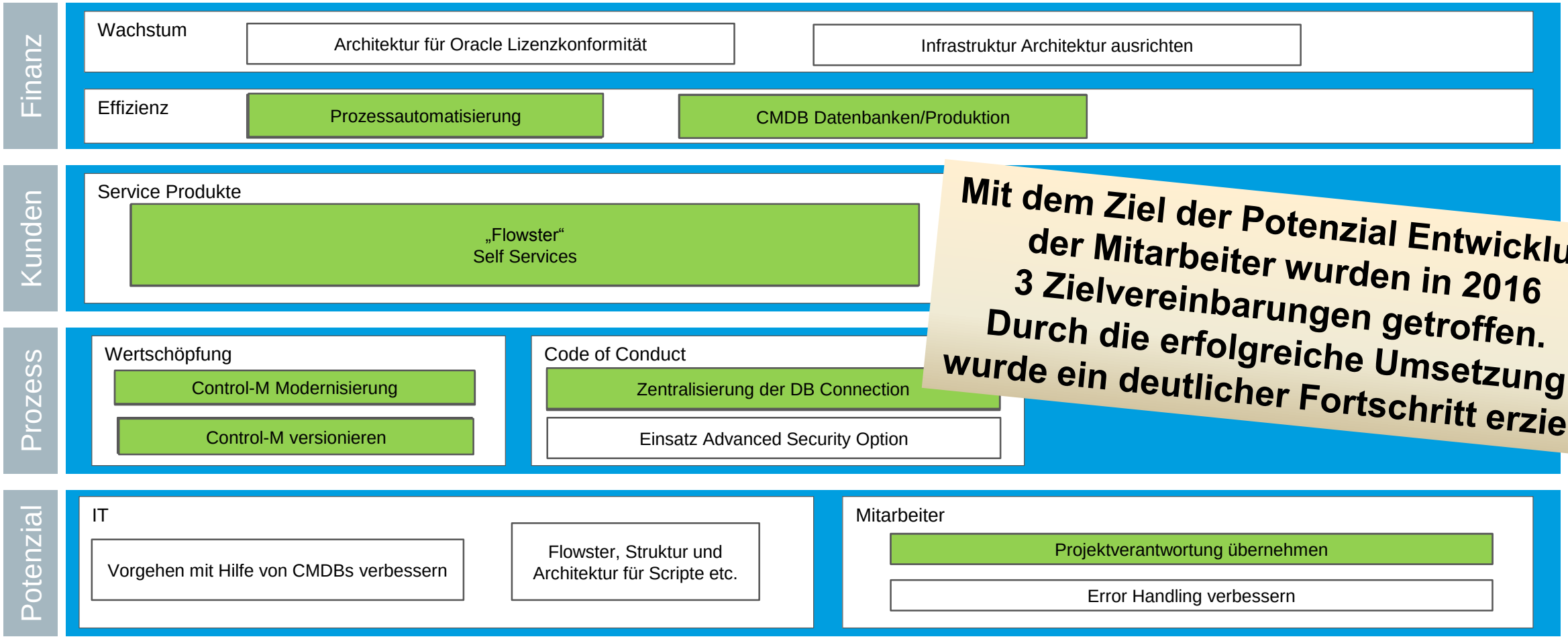




Automation (Building Pipeline)

Barmenia Versicherungen

Das Zielbild für Mitarbeiter detaillieren und sie integrieren!



Mit dem Ziel der Potenzial Entwicklung der Mitarbeiter wurden in 2016 3 Zielvereinbarungen getroffen. Durch die erfolgreiche Umsetzung wurde ein deutlicher Fortschritt erzielt!

Barmenia Versicherungen

Vortragsinfos

- Was bedeutet Compliance zu Zeiten von Digitalisierung (für Versicherungen) und was muss man dafür alles tun?
- Warum spielt die IT-Strategie im Kontext von DSGVO und VAIT eine wichtige Rolle und wie sorgt man für zielgerichtetes Handeln aller Beteiligten?
- **Warum ein Cloud Ansatz auch für Compliance Lösungen hilfreich sein kann.**
- Wie kann Compliance mehr Chance als nur Kosten sein?

Zukunftsvision für die Barmenia Produktion

- Entwicklung zum Private Cloud Provider
- Konsequente Vollautomation
  - Nutzen der GUI ist grundsätzlich zu vermeiden!
  - Zentrales Scheduling mit Control-M
  - Automatisches Deployment und Patching
  - Self Service Portal für alle Wiederkehrenden Arbeiten (Rechtevergabe, Deployments etc.)
- SLA Management und Reporting
- Toolset für DevOps / DataOps Support
  - GIT, ansible, building pipeline
  - Docker, OpenShift
  - Data as a Service per Actifio
- Configuration Management (CMDB)
- Compliance Management
  - Auditing aller Änderungen
  - Change nur über Ticket

Bild: TDMPHARMA

Barmenia Versicherungen

Warum ein Cloud Ansatz auch für Compliance Lösungen hilfreich sein kann

Gründe für Cloud Nutzung

- Es soll von überall aus (mobil) gearbeitet werden.
- (DevOps)Teams benötigen ad hoc neue Systeme.
- Es werden RDBMS angefordert, die bisher nicht im Einsatz sind.
- Durch Virtualisierung explodiert die Anzahl der Systeme und sind nicht mehr „mit der Hand“ zu administrieren.
- Man verfügt über zu wenig eigene Mitarbeiter/innen für die Administration der Menge der benötigten Systeme.
- Es fehlen Self Service Portale und Automatismen.

Weil die Lösungen der Cloud Technologie auch Lösungen für Compliance Probleme sind!

Übersicht Infrastruktur Stack

Tools

Monitoring/Diagnostic

graylog

pingdom

Check_MK

Quest FOGLIGHT

Continous Delivery

Provisionierung

sonarqube

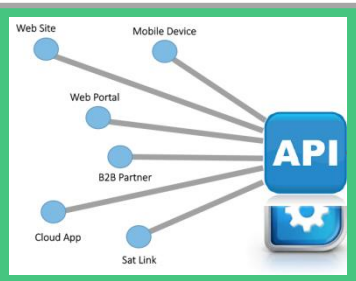
Jenkins

bmc

Ruby

puppet

Platform as a Service (PaaS)



API Gateway

IAM

Omada

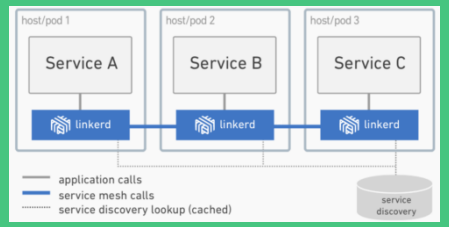
Micro Services

Nano Services

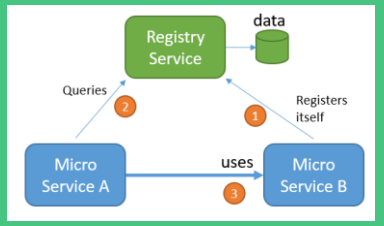
DB Services (DBaaS)

MESOS

DC/OS



Delivery

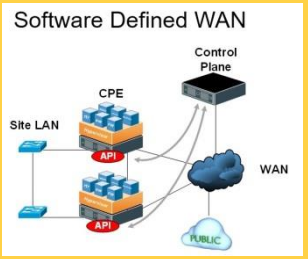


FLOWSTER IT AUTOMATION SOFTWARE

RDBMS

Container as a Service (CaaS)

Infrastructure as a Service (IaaS)



Data as a Service (DaaS)

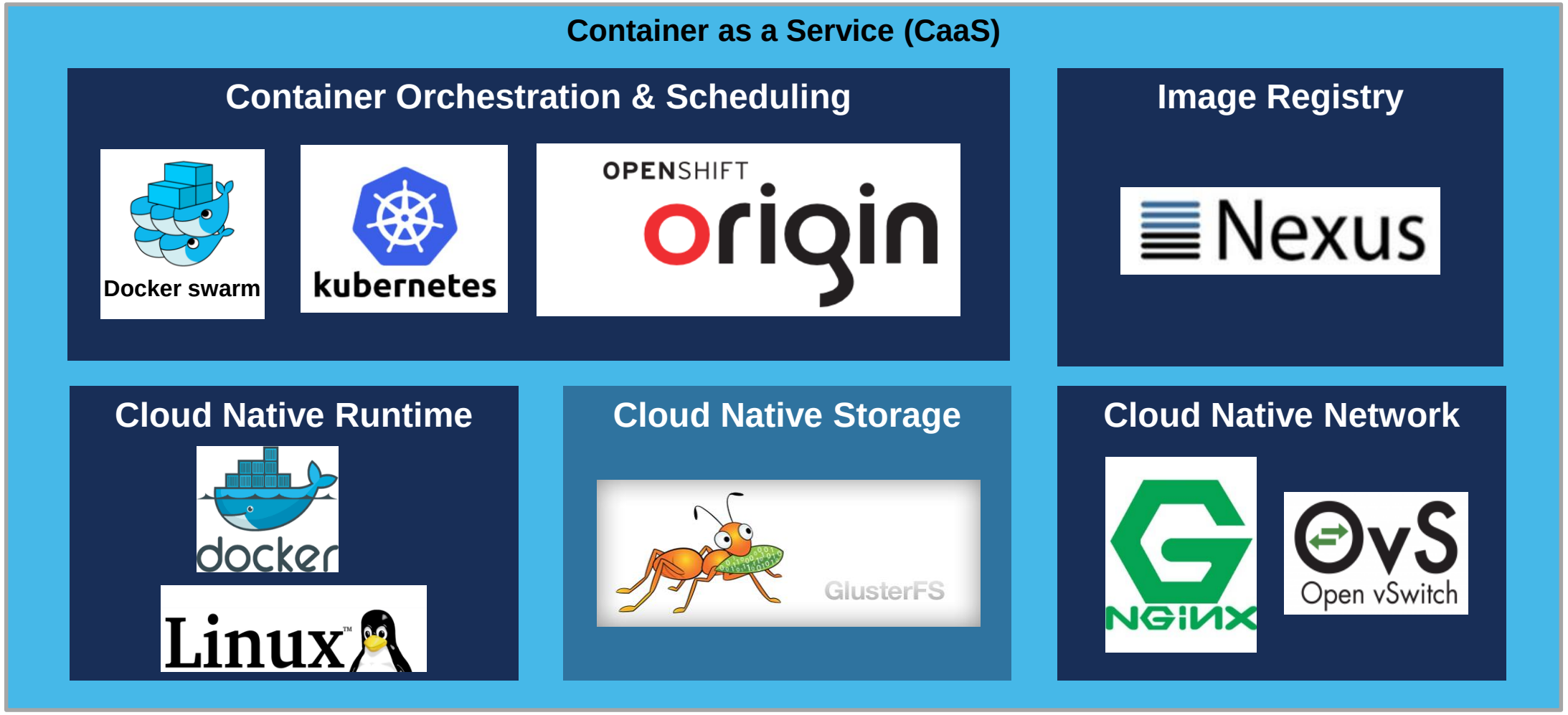
Storage

actifio

Quelle Javamagazin 11/2017
Dr. Josef Adersberger

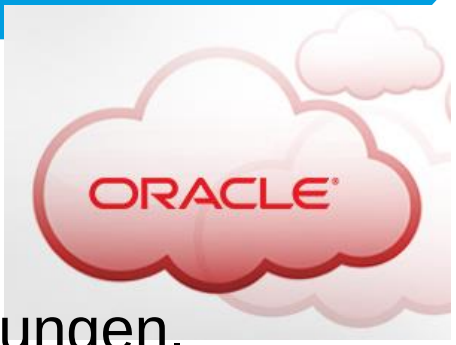
Barmenia Versicherungen

Wie könnte ein Container Stack aussehen?



Barmenia Versicherungen

Was leistet ein (Oracle) Cloud Services nicht?



- Die Definition, welcher Service für wen der Richtige ist.
- Wer auf welche Daten Zugriff bekommt bzw. bekommen darf.
- Die Voraussetzungen für verteilte Transaktionen über mehrere Anwendungen.
- Welche Performance- und Datenschutzaspekte zu berücksichtigen sind.
- Einen „Helpdesk“ für die Nutzer der Cloud.
- Eine gute Anbindung an das Active Directory (Benutzer, Gruppen etc.).
- Verfügbarkeit entsprechend der eigenen Erwartung.
  (zumindest bis jetzt ist das noch nicht brauchbar).
- Sicherstellung der Funktionsfähigkeit von Anwendungen mit der Infrastruktur im Kontext von Upgrades/Patches.
- Kostenkontrolle (ist noch nicht transparent genug).

Barmenia Versicherungen

Cloud Problem „Datenschutz“
USA – Deutschland (EU)

Datenschutz – USA vs Deutschland (Europa)

	USA	Deutschland
Bedeutung	Teil des Verbraucherschutzrechts	Grundrecht
Recht	Kein branchenübergreifendes Datenschutzgesetz	Bundesdatenschutzgesetz (ab 2018 Europäische Datenschutzgrundverordnung)
Aufsicht	Federal Trade Commission (FTC)	Bundes- und Landesbeauftragte für Datenschutz
Datenvergabe	Selbstregulierung durch Wirtschaft und Privatpersonen	Informationelle Selbstbestimmung (Grundrecht)
Datenschutz & Terrorabwehr	Patriot Act erlaubt FBI, NSA oder CIA Zugriff ohne richterliche Anordnung auf Server von US-Unternehmen	Grundsätzlich richterliche Anordnung nötig sowie Informationspflicht der Behörden gegenüber Betroffenen

Quelle
Datenschutzkongress 2016

Cloud in USA und DSGVO? Das passt nicht!

Beispiel aus der Leistungsbeschreibung der Oracle Cloud

10. Datenschutz

10.1 ***Oracle wird bei der Erbringung der Services die Oracle Services Privacy Policy einhalten***, die unter http://www.oracle.com/html/Services-privacy-policy.html eingesehen werden kann und die durch Verweis Teil dieses Vertrags wird.
Oracle behält sich nach eigenem Ermessen Änderungen an der Oracle Services Privacy Policy vor; ***Oracle wird*** jedoch ***die*** durch die Richtlinie ***definierten Schutzmaßnahmen für Ihre persönlichen Daten***, die Teil Ihrer Inhalte sind, während des Leistungszeitraums Ihres jeweiligen Auftrags ***nicht wesentlich reduzieren***.

Barmenia Versicherungen

Vortragsinfos

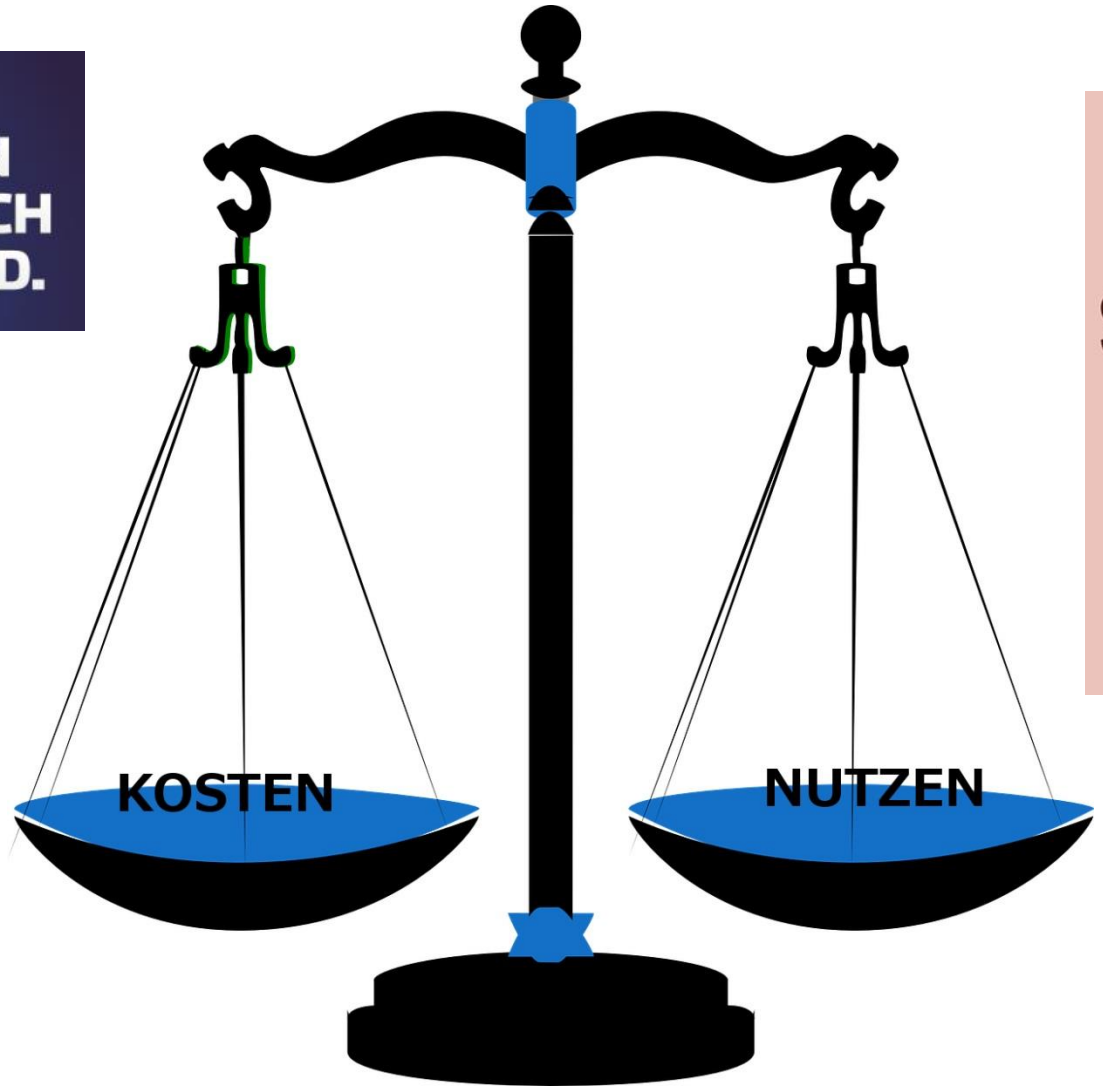
- Was bedeutet Compliance zu Zeiten von Digitalisierung (für Versicherungen) und was muss man dafür alles tun?
- Warum spielt die IT-Strategie im Kontext von DSGVO und VAIT eine wichtige Rolle und wie sorgt man für zielgerichtetes Handeln aller Beteiligten?
- Warum ein Cloud Ansatz auch für Compliance Lösungen hilfreich sein kann.
- **Wie kann Compliance mehr Chance als nur Kosten sein?**

Wie kann Compliance mehr Chance als nur Kosten sein?

PROBLEME KANN MAN NIEMALS MIT DERSELBEN DENKWEISE LÖSEN, DURCH DIE SIE ENTSTANDEN SIND.
Albert Einstein

✓ **proaktiv**

☐ ~~**reaktiv**~~

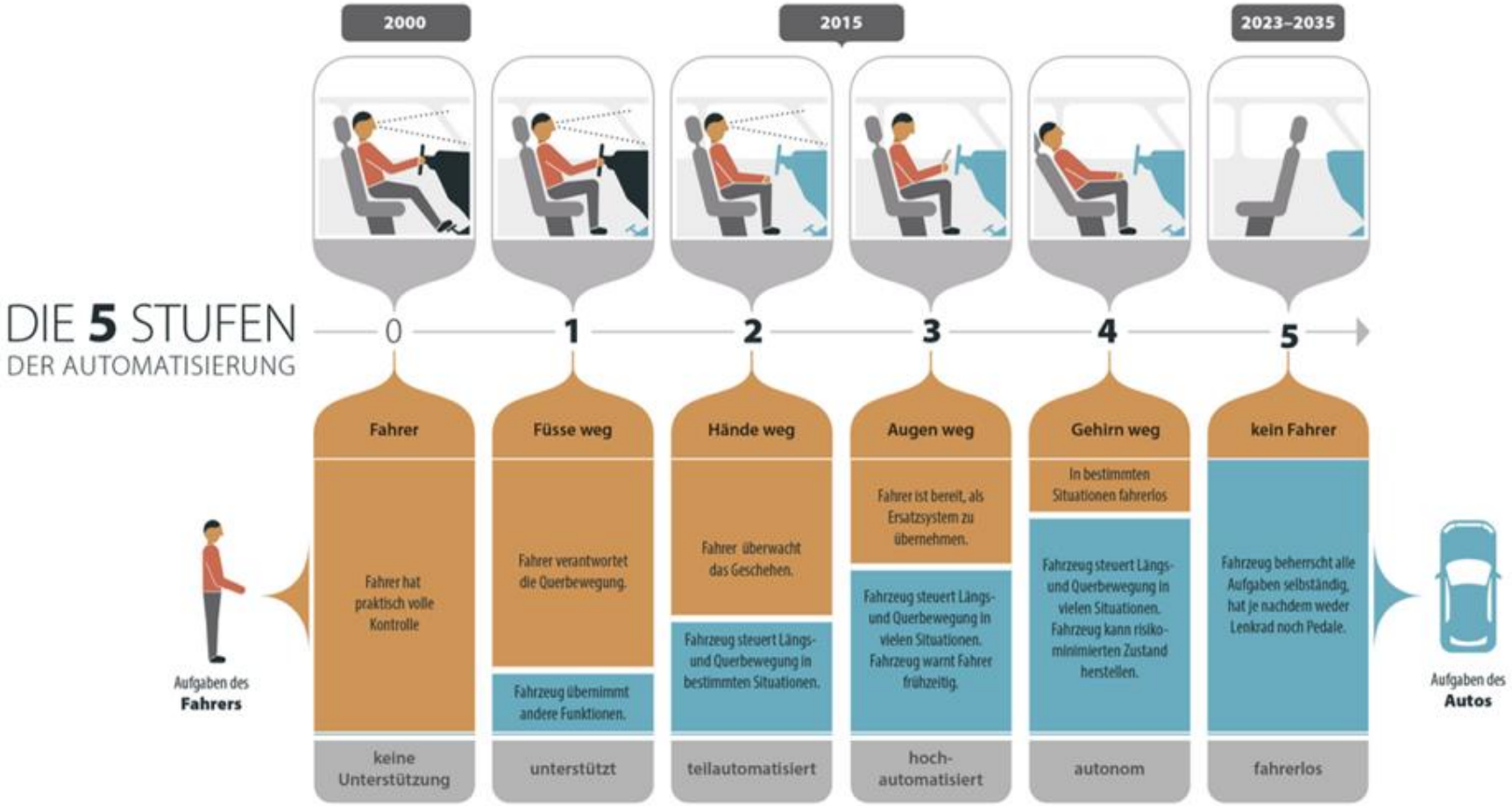


INNOVATION IST KEINE GARANTIE GEGEN DAS SCHEITERN, ABER OHNE INNOVATION IST DAS SCHEITERN GARANTIERT.

STEFAN R. MUNZ

Barmenia Versicherungen

Die 5 Stufen der Automatisierung am Beispiel „Auto fahren“



Barmenia Versicherungen

Beispiel „autonomes Fahren“

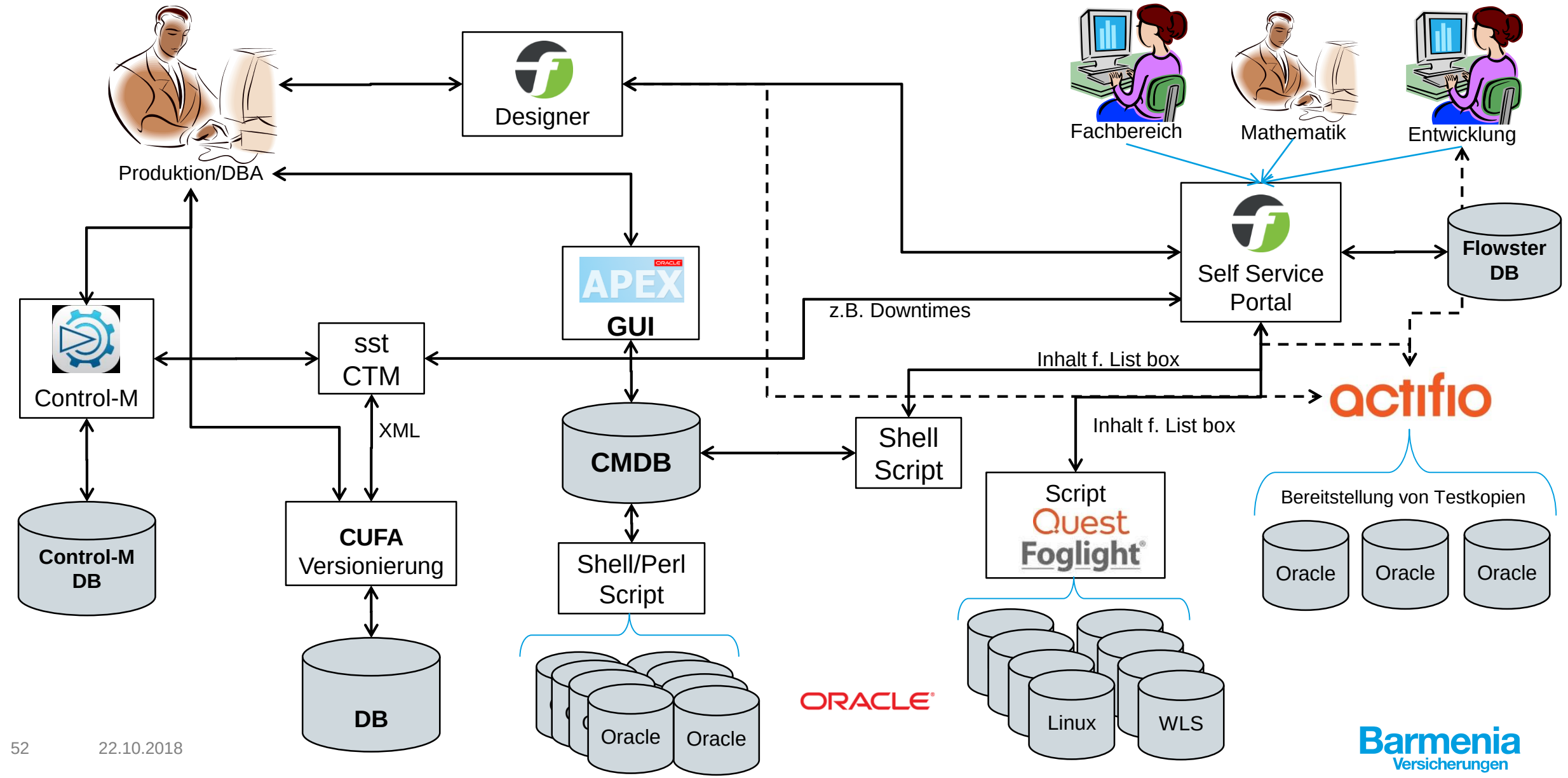
Gartner schätzt, dass bis 2020 werden rund eine 250 Millionen vernetzte Fahrzeuge weltweit auf den Straßen unterwegs sein werden.
Die Prognose des Marktforschungs-unternehmens Gartner stammt aus einer Studie über das Internet der Dinge.

Heute geht man davon aus, dass alle Fahrzeuge im Umkreis von 800 - 1.000 Metern per WLAN vernetzt werden können. Reaktionen wie bremsen, ausweichen etc. sind damit in wenigen Millisekunden koordinierbar.

Quelle: www.car-it.com

Barmenia Versicherungen

Private Cloud Beispiele der Barmenia
Übersicht des (neuen) Produktionsumfeldes der Barmenia

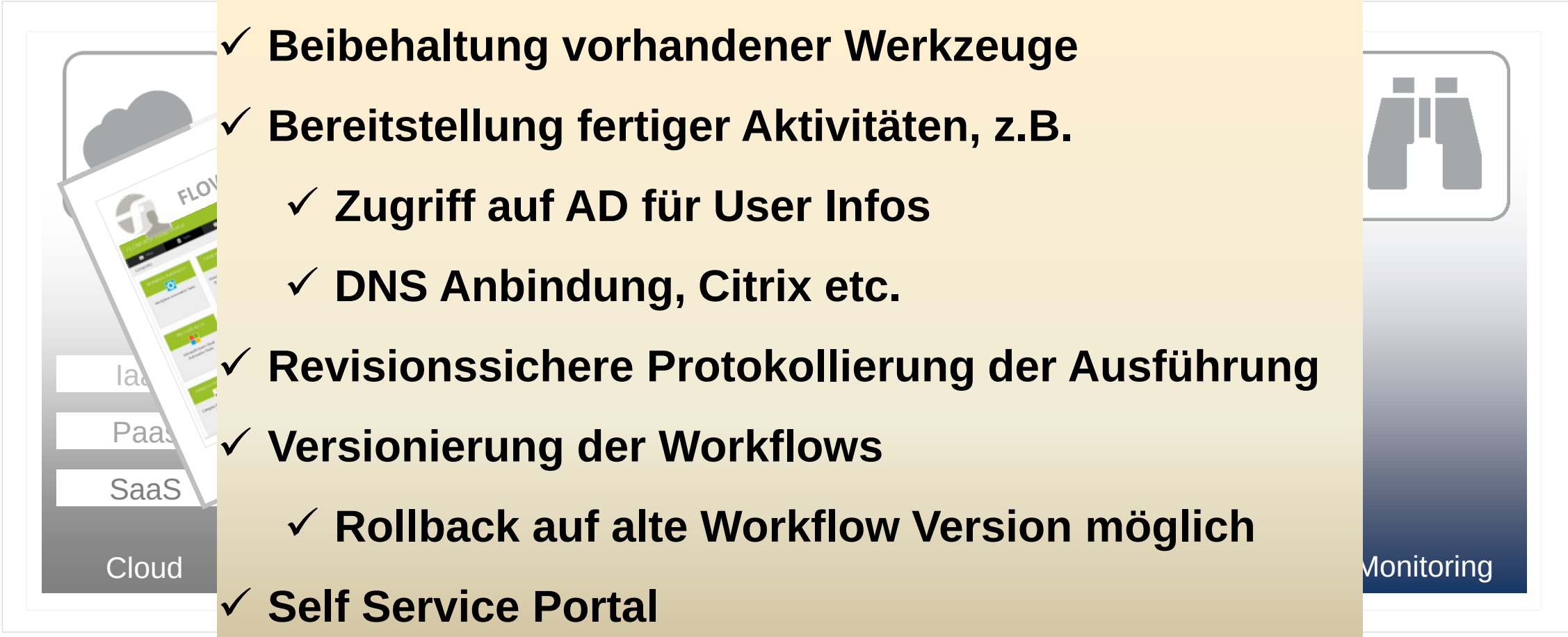


Barmenia Versicherungen

Private Cloud Beispiele der Barmenia
Prozessautomation mit Self Services

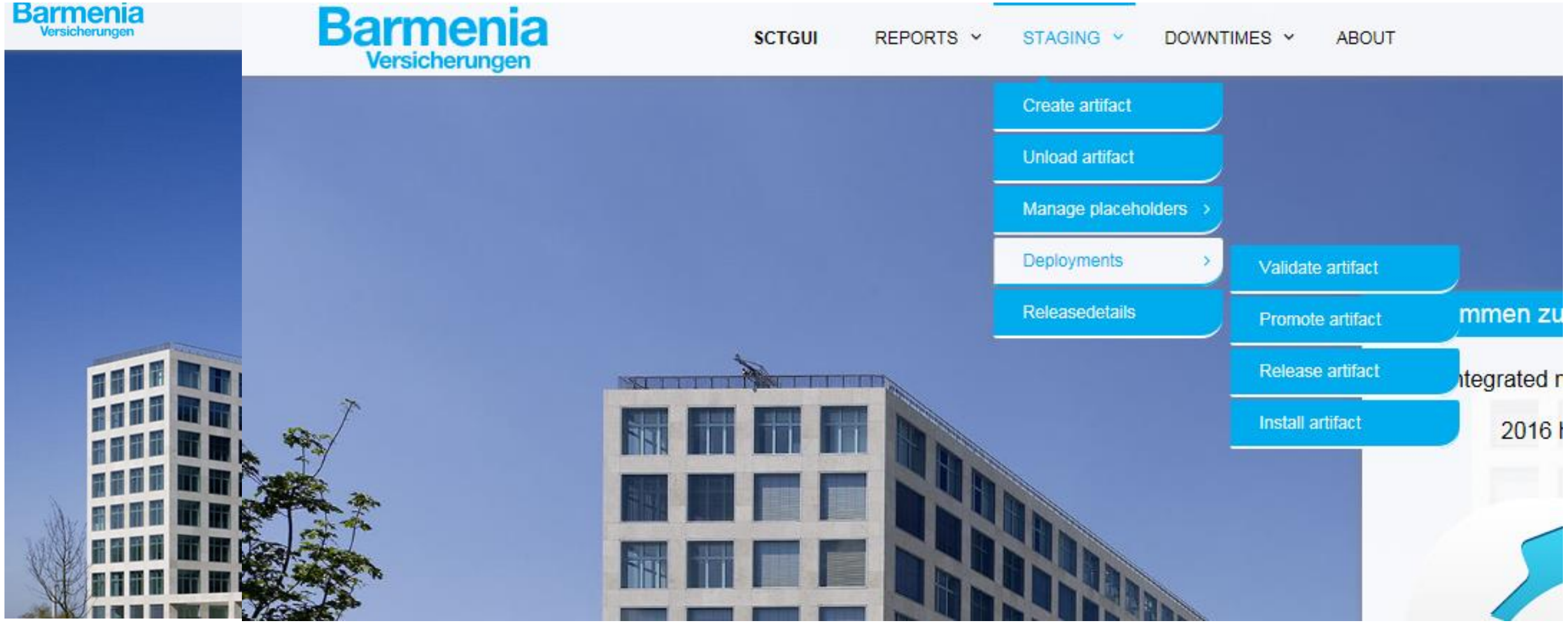
Cloud

Rechenzentrum



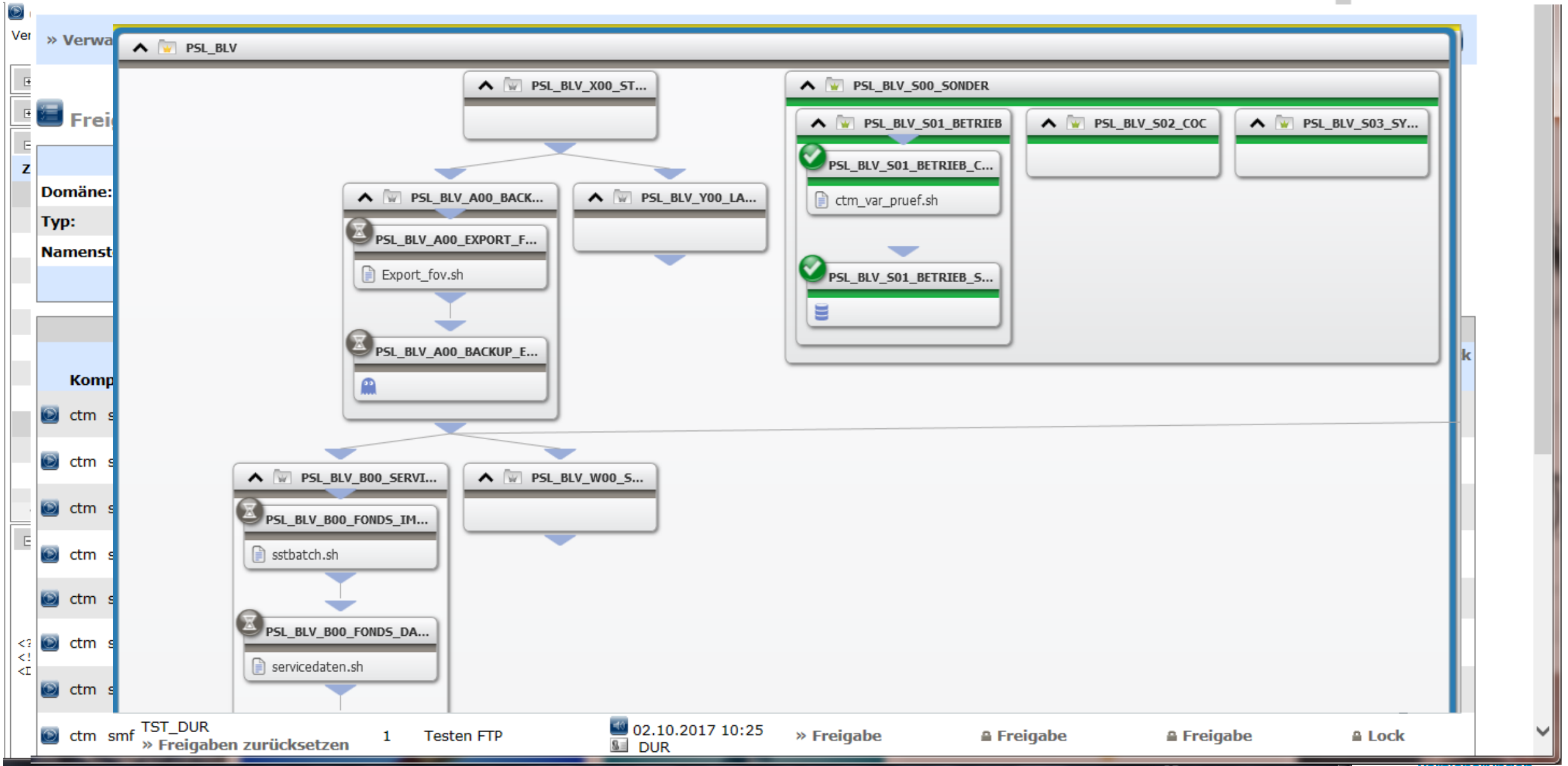
- ✓ **Beibehaltung vorhandener Werkzeuge**
- ✓ **Bereitstellung fertiger Aktivitäten, z.B.**
  - ✓ **Zugriff auf AD für User Infos**
  - ✓ **DNS Anbindung, Citrix etc.**
- ✓ **Revisionssichere Protokollierung der Ausführung**
- ✓ **Versionierung der Workflows**
  - ✓ **Rollback auf alte Workflow Version möglich**
- ✓ **Self Service Portal**

Private Cloud Beispiele der Barmenia
Selbst erstellte Schnittstelle für Automation mit Control-M

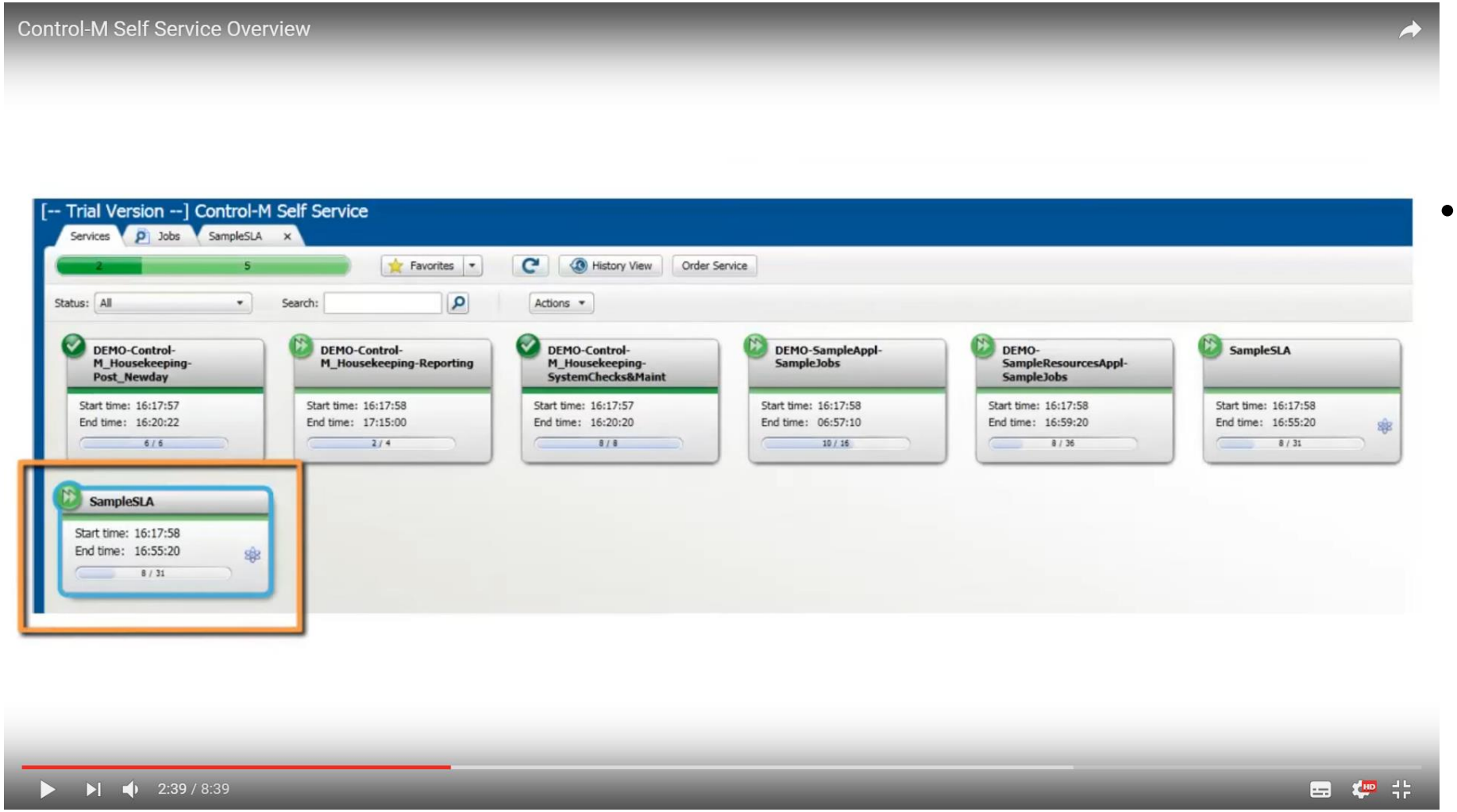


Barmenia Versicherungen

Private Cloud Beispiele der Barmenia
Revisionssichere Versionierung von Jobs



Private Cloud Beispiele der Barmenia
Control-M Self Services Portal für Kunden

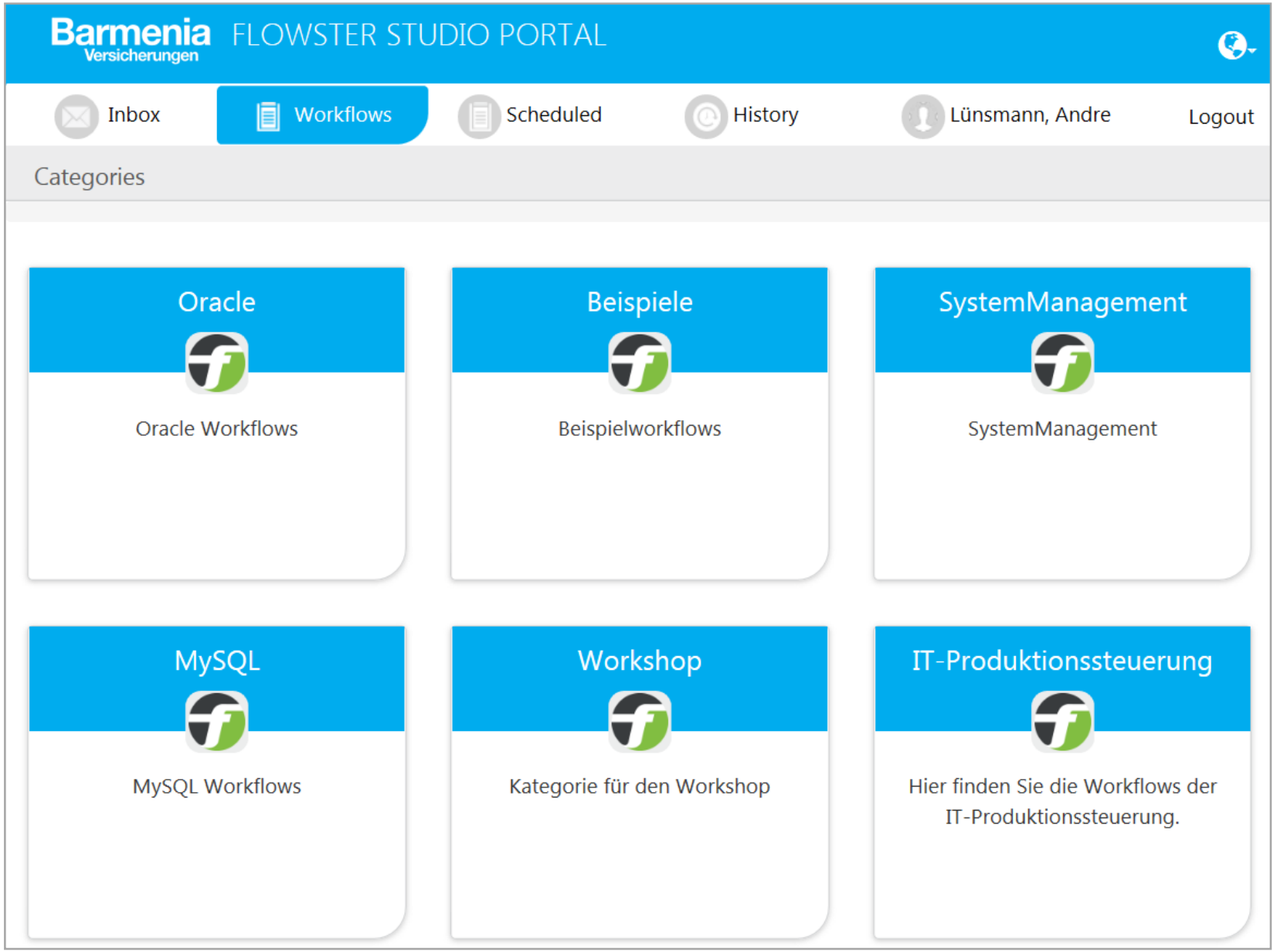


- Der Fachbereich kann Jobs prüfen, freigeben und selber (weiter)laufen lassen

Lizenzpflichtig!

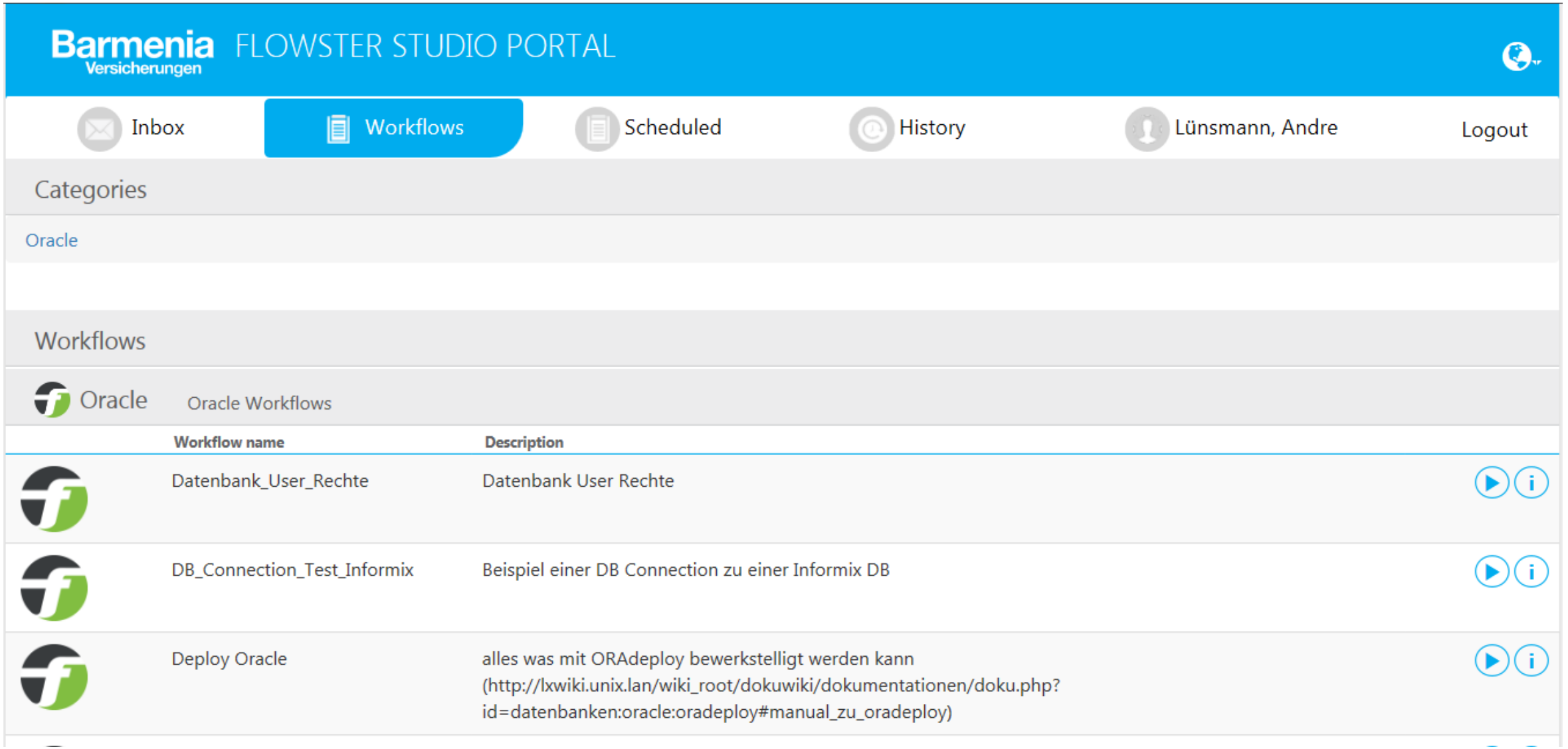
Barmenia Versicherungen

Private Cloud Beispiele der Barmenia
Self Service Portal – Kategorien –



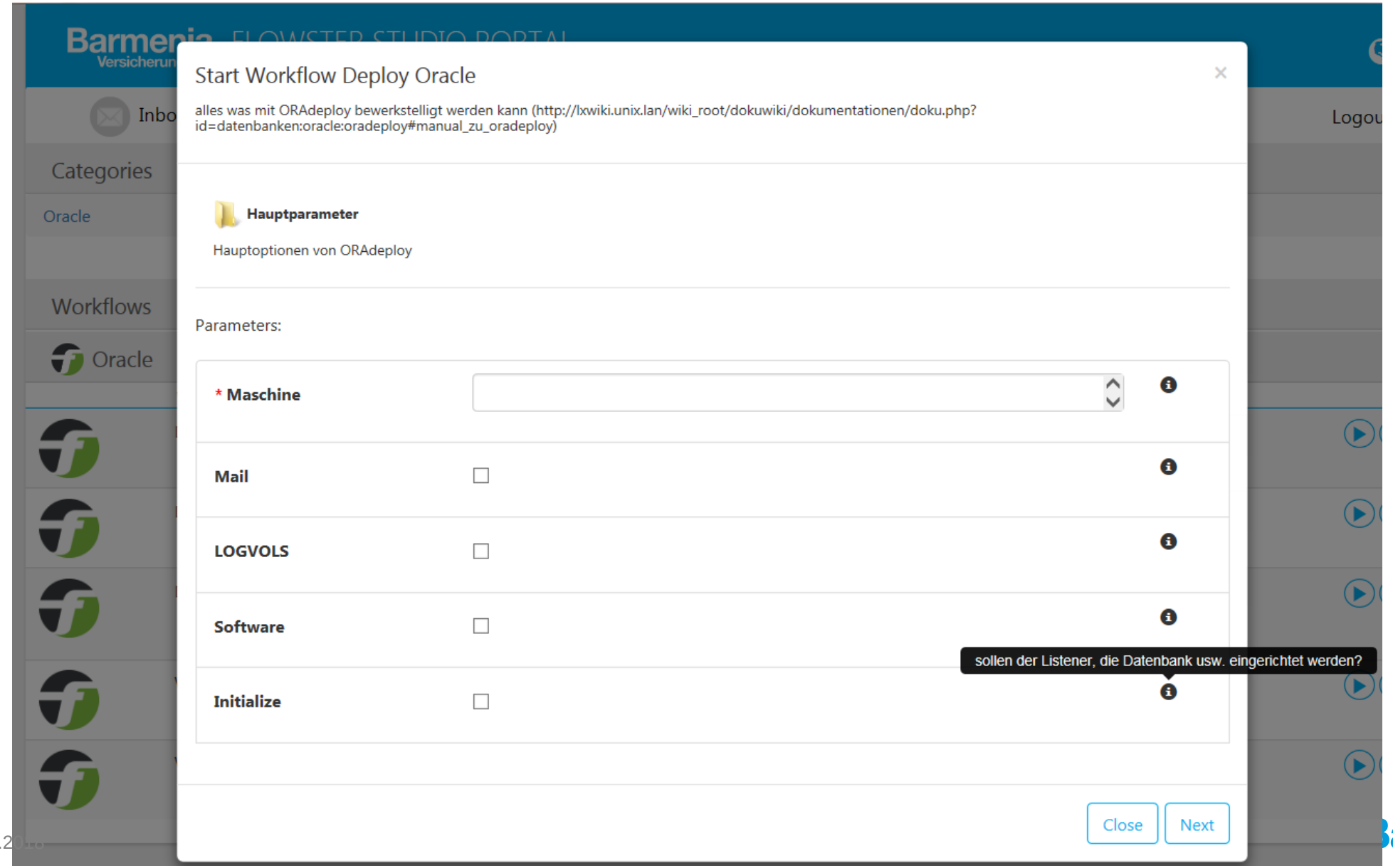
Barmenia Versicherungen

Private Cloud Beispiele der Barmenia
Self Service Portal – Workflows –



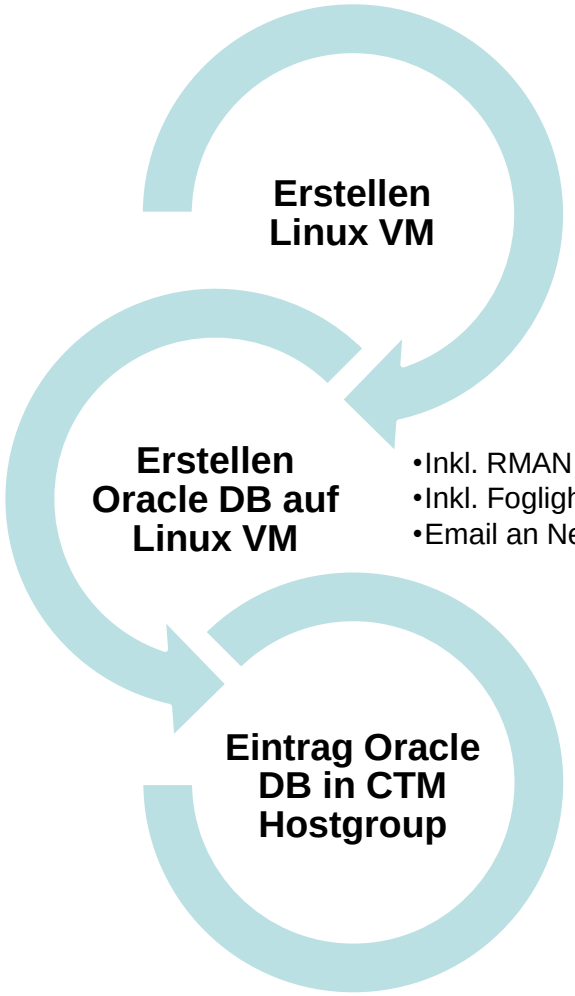
Barmenia Versicherungen

Private Cloud Beispiele der Barmenia
Self Service – Wizard –



Barmenia Versicherungen

Private Cloud Beispiele der Barmenia
Self Service – Deploy Oracle–



- Inkl. CTM Agent
- Inkl. Foglight Agent
- Inkl. Check_mk Agent

- Inkl. RMAN Katalog Eintrag
- Inkl. Foglight DB Überwachung
- Email an NetBackup Admins

- Tägl. NetBackup Full Backup per CTM
- Alle 6 Minuten Archive Logs Prüfung mit mind. stündlicher Archivierung
- Tägl. Cleanup Job TAR Files
- Wöchentl. Cleanup RMAN Repository
- Regelm. Cleanup Job mit Backup der FRA

Barmenia Versicherungen

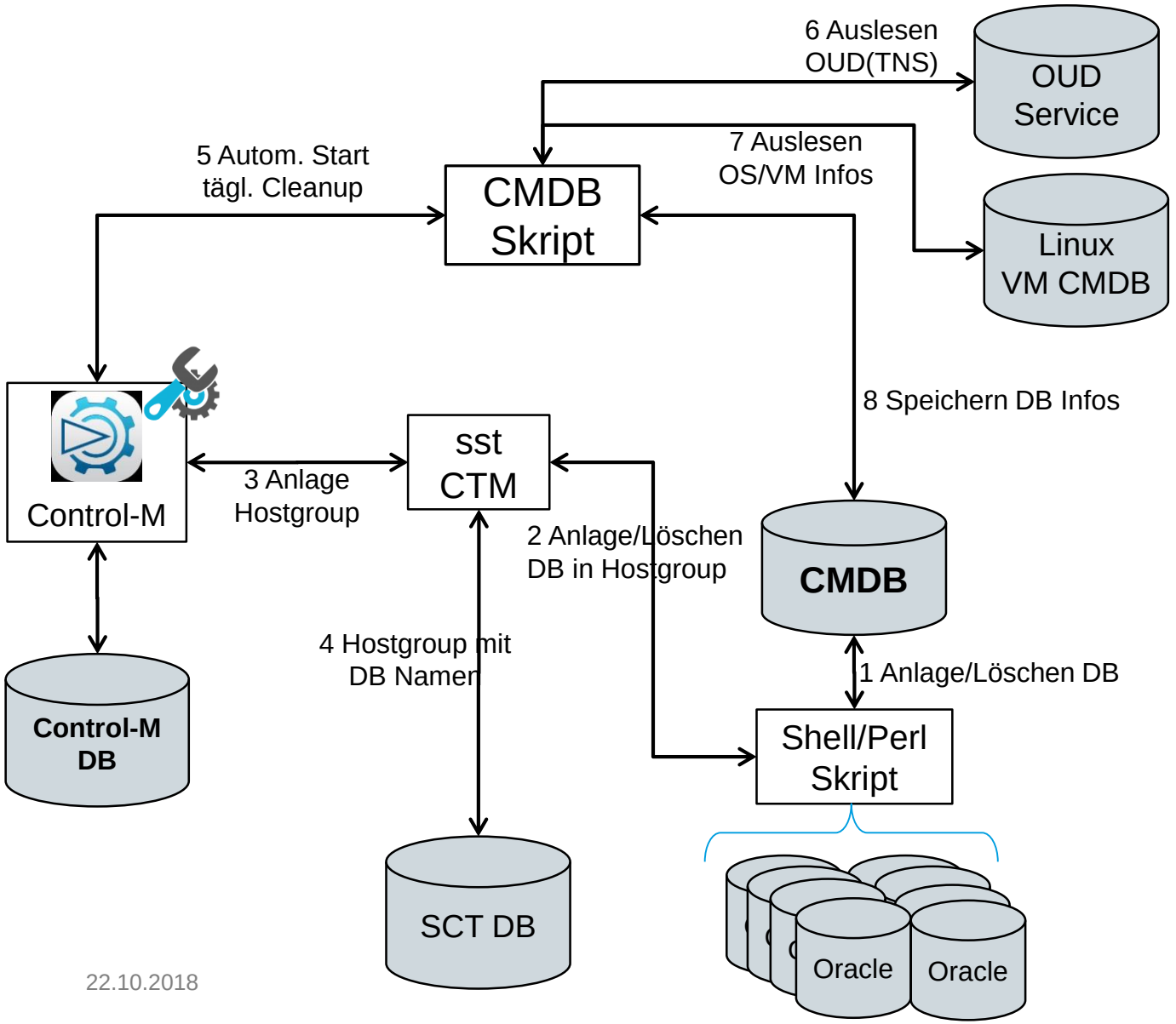
Private Cloud Beispiele der Barmenia
Aufbau von Configuration Management Datenbanken als Basis

Was ist die Basis?

- SQLs die per Scheduler regelm. laufen
- APEX erzeugte Oberfläche
- Zulieferung aus dem VM Umfeld per Quest Foglight Skript

Barmenia Versicherungen

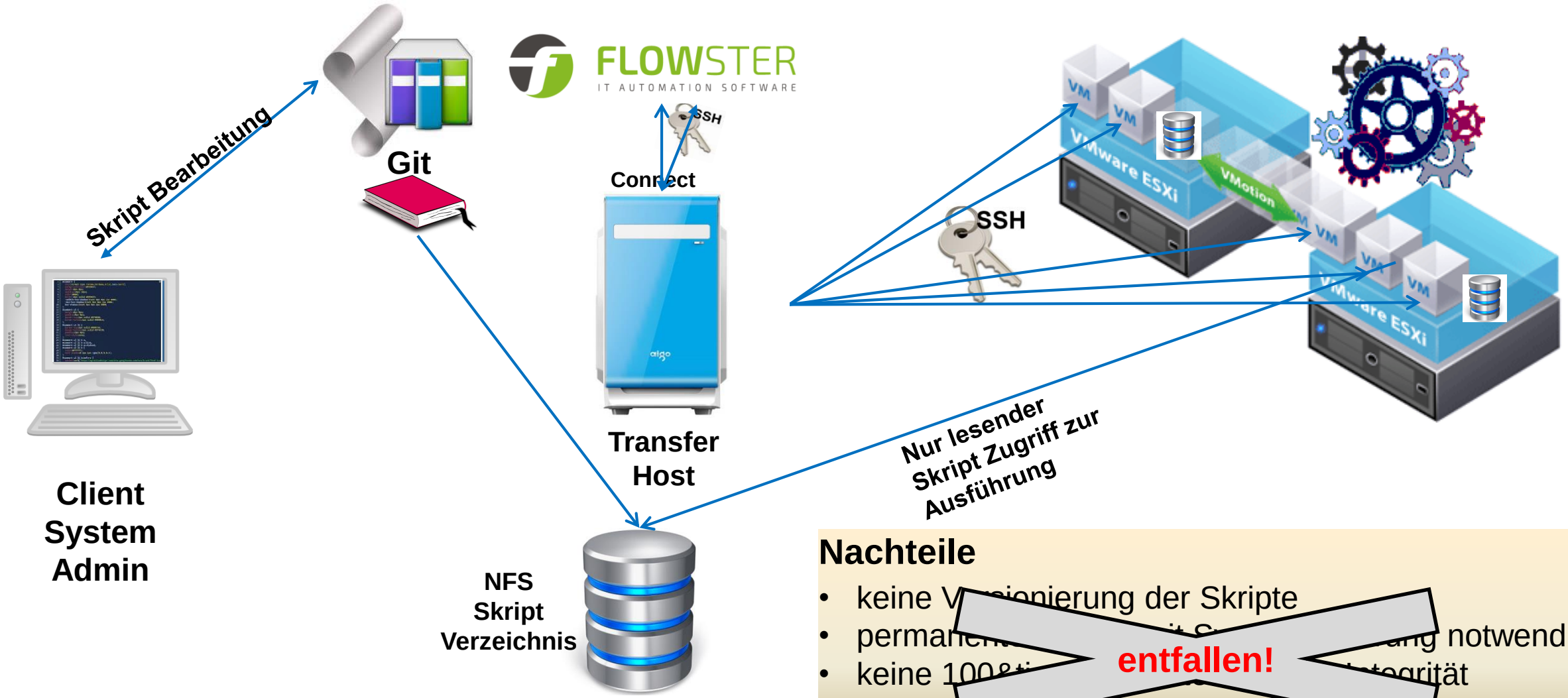
Zentrale Pflege der DB Systeme



1. Anlegen/Löschen DB System
2. Beauftragung Anlage/Löschen Hostgroup bzw. DB in Hostgroup
3. Anlage Anlage/Löschen Hostgroup in Control-M
4. Anlage Anlage/Löschen DB in Hostgroup in SCT-DB
5. Tägl. Cleanup Job
6. Auslesen OUD/TNS Services
7. Auslesen OS/VM Infos aus der Linux VM CMDB
8. Aktualisierung der DB CMDB

Barmenia Versicherungen

Administrationsprinzip zentrale Änderung, Nachweispflichten



Nachteile

- keine V[illegible]ionierung der Skripte
- permanent[illegible] notwendig
- keine 100%i[illegible]tegrität
- Nachwe[illegible]über Logfile Archivierung [illegible]portsafe

entfallen!

Barmenia Versicherungen

Private Cloud Beispiele der Barmenia
Revisionssicherer Ausführungsreport von Flowster

Wf Name	Wf Description	Started by	Started at	Finished at	Overall Status	Approval Status	Comments
Deploy Oracle	alles was mit ORAdeploy bewerkstelligt werden kann (http://lxwiki.unix.lan/wiki_root/dokuwiki/dokumentationen/doku.php?id=datenbanken:oracle:oradeploy#manual_zu_oradeploy)	IDM\037478	4/7/2017 2:18:38 PM	4/7/2017 2:50:23 PM	Deploy Oracle completed		User ip address is 172.20.202.143

Parameters:
Maschine=lxu5j.barmenia.lan
Mail=True
LOGVOLS=True
Software=True
Initialize=True
WF_Nutzer=idm\037478
Version=12102_161018
DB_Name=ZFKP
DGSIDE=
LOGVOLSIZE=16000
ADDFRASIZE=3000
CHARSET=WE8ISO8859P15
NATCHARSET=AL16UTF16
Compatibility=
DBPORT=
Template=BARM_12c_general.dbt
DGS2HOST=
RCVFDSIZE=6500

Barmenia Versicherungen

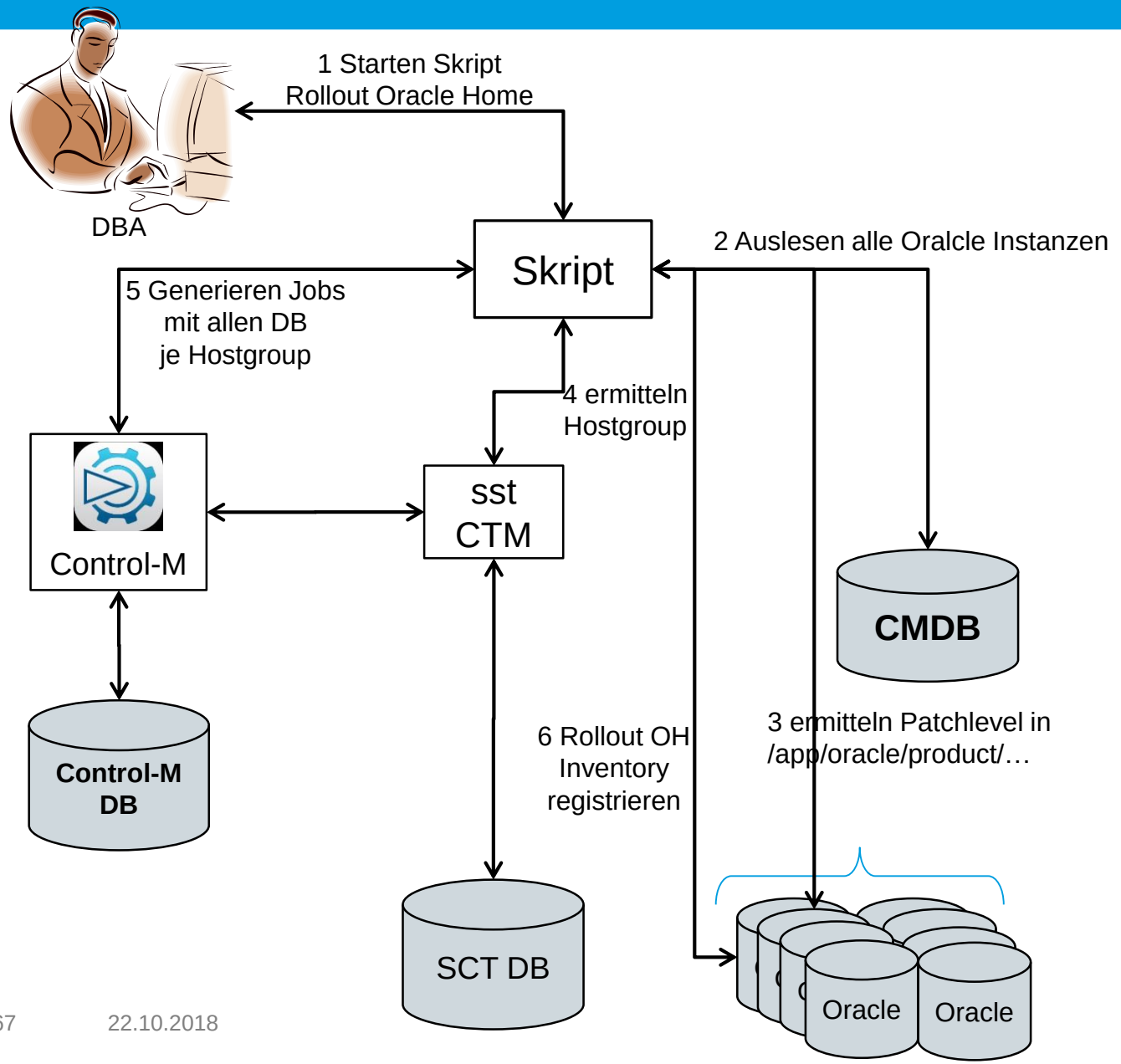
Datenbank Patch: prinzipielle Vorgehensweise

1. Image erstellen
2. Image im „Repository“ bzw. auf NFS ablegen
3. Image gruppenweise auf Hosts ausbringen
4. ORACLE_HOME gruppenweise umswitchen
5. Datapatch aufrufen
6. Patchinstallation prüfen

(Servcie)Bildung für CTRL-M Hostgroups

- Die Gruppenbildung basiert auf
  - fachlich zusammengehörige Instanzen die gleichzeitige Wartungsfenster haben
  - Trennung von Anwendungen mit hauptsächlich internem Belang von Anwendungen mit hauptsächlich externem Belang
- Es sind maximal 8 DB-Rechner in einer Gruppe, weil
  - alle Instanzen parallel „gepachted“ werden
  - die Gruppe in < 15 Minuten fertig sein soll
- Der Patch dauert derzeit ca. 6-7 Minuten pro Gruppe

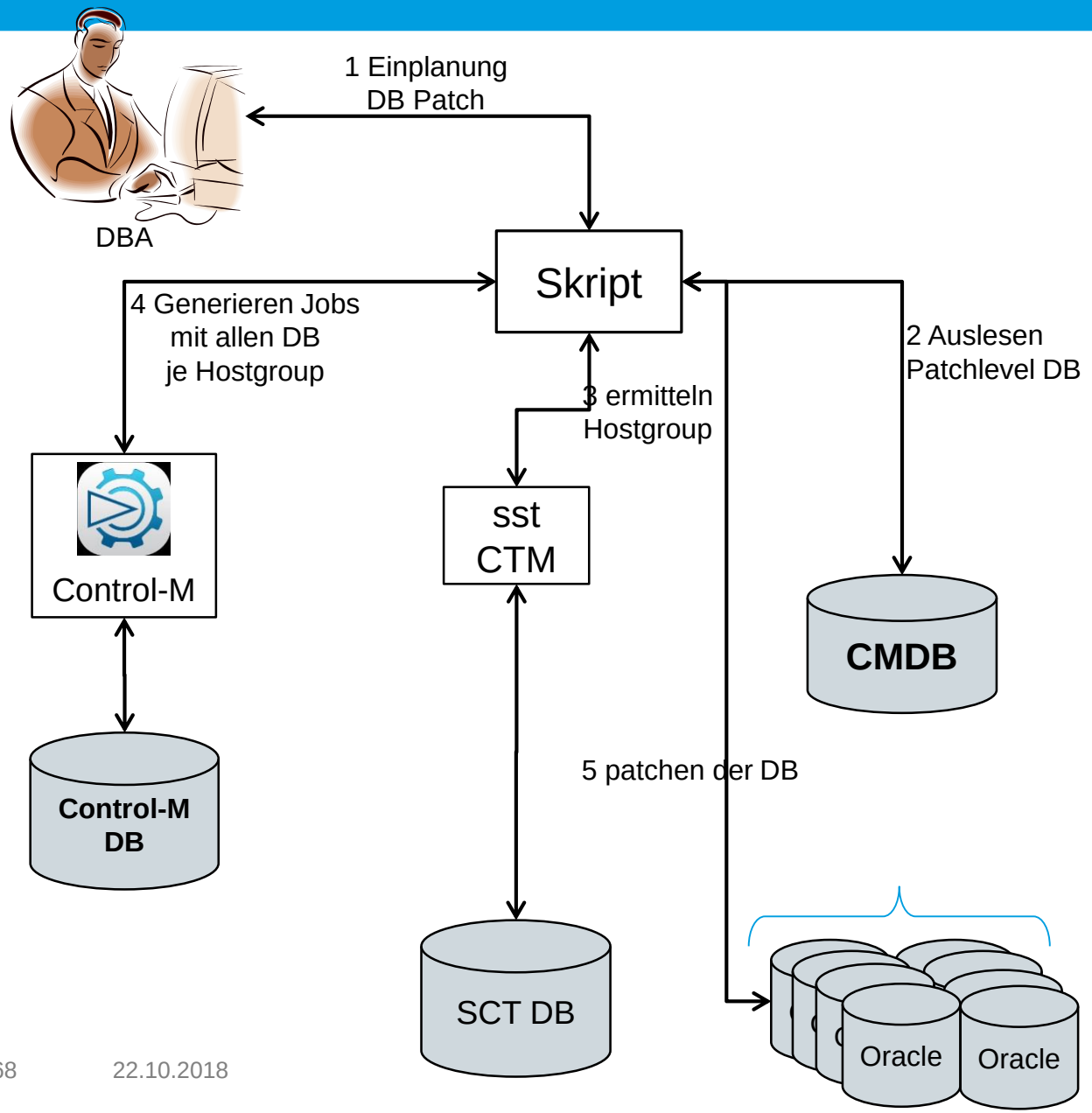
Rollout neues Oracle Home



1. Start Rollout Skript Oracle Home
2. Auslesen aller Oracle Instanzen
3. Ermitteln Patchlevel auf Zielsystem
4. Ermitteln Hostgroups
5. Generieren Jobs für alle DB je Hostgroup
6. Rollout neues Oracle Home
   - FS anlegen
     - Größe in Konfigurationsdatei vermerkt
   - TAR-Image aus „Repository“ holen und entpacken
   - neues ORACLE_HOME in Inventory registrieren

Barmenia Versicherungen

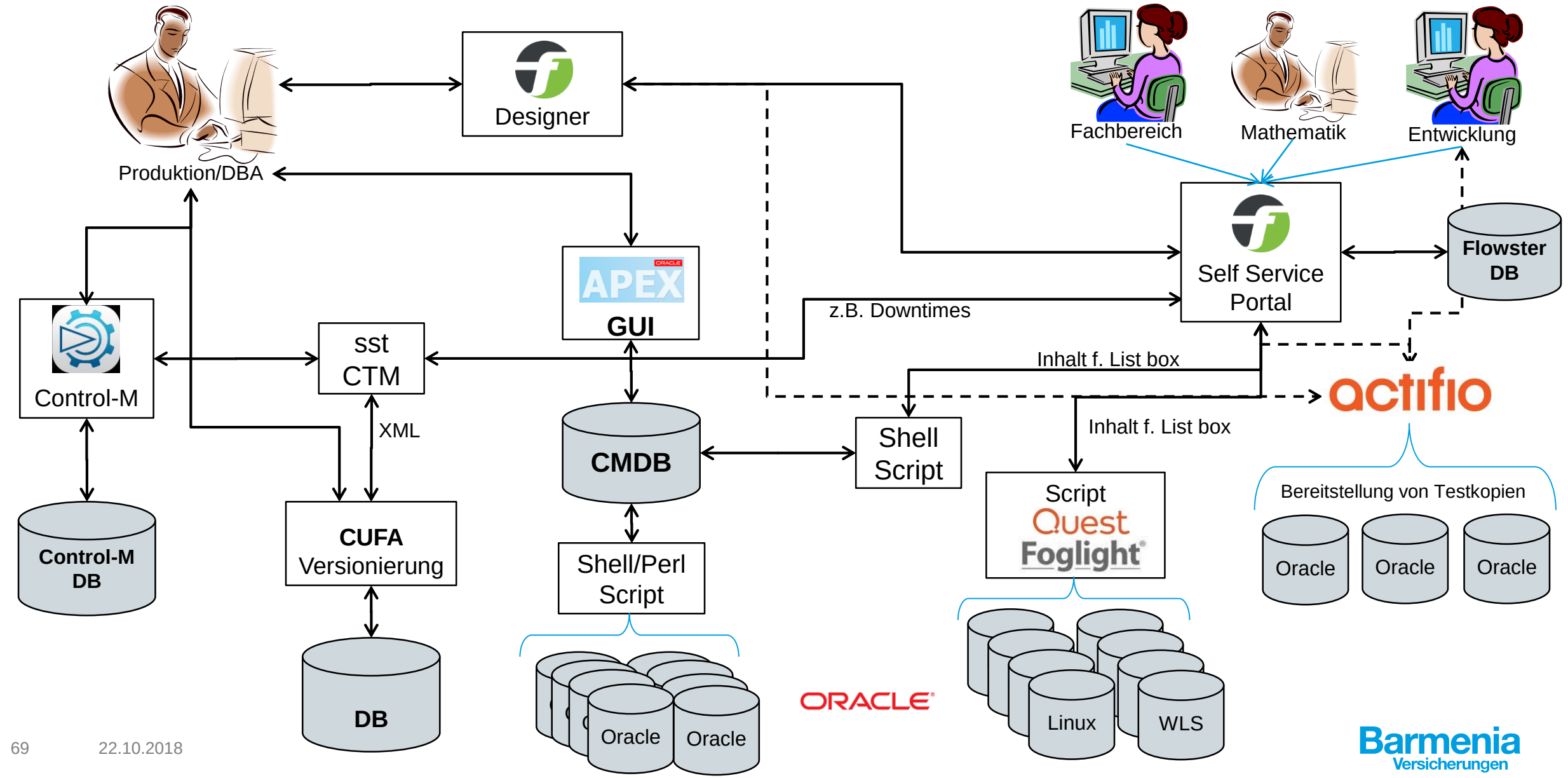
Patch der Datenbanken



1. Einplanen des DB Patch
2. Auslesen der Patchlevel
3. Ermitteln der Hostgroup
4. Generieren der Jobs mit allen DB je Hostgroup
5. Patchen der DB Instanz
   - evtl. störende alte Patches deinstalliert
   - die Instanz herunterfährt
   - Den Listener herunterfährt
   - die Umgebung auf das neue OH setzt und daraus die Instanz und den Listener startet
     - listener.ora wird angepasst
   - datapatch aufruft
   - Erfolgreichen Patch testen

Barmenia Versicherungen

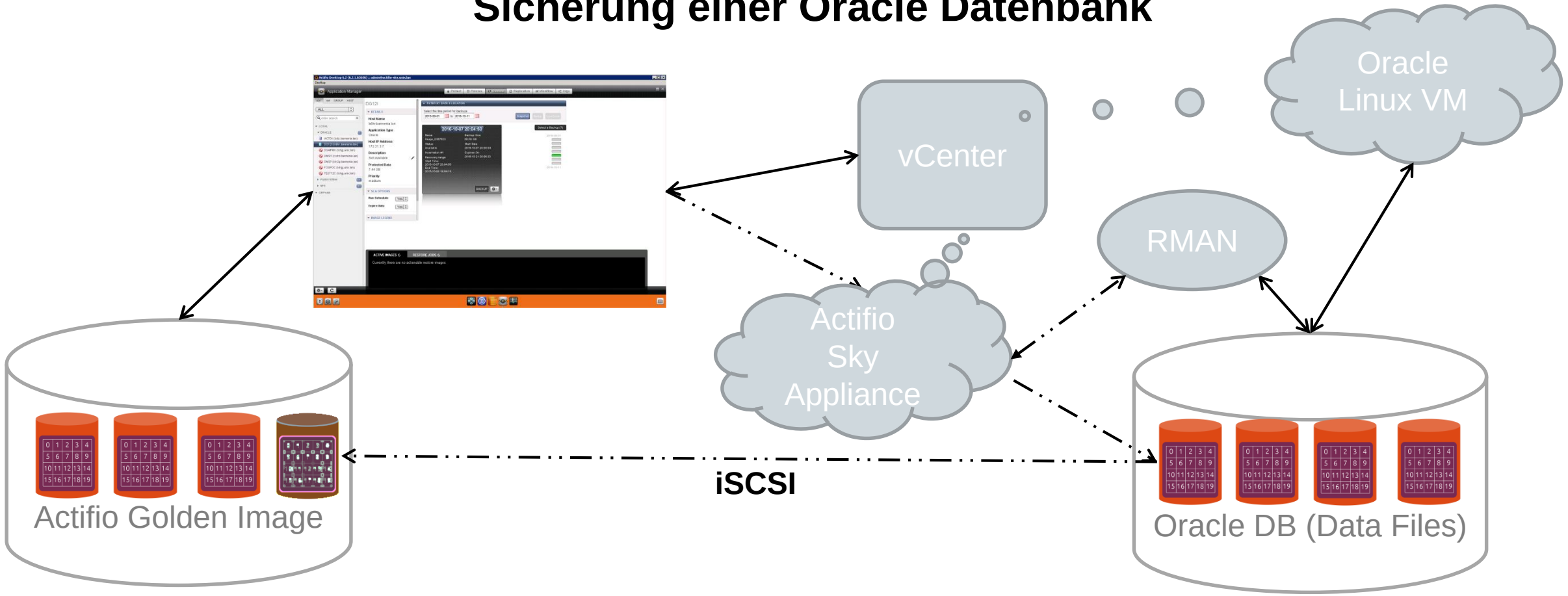
Data as a Service mit actifio



Barmenia Versicherungen

DB as a Service mit Actifio

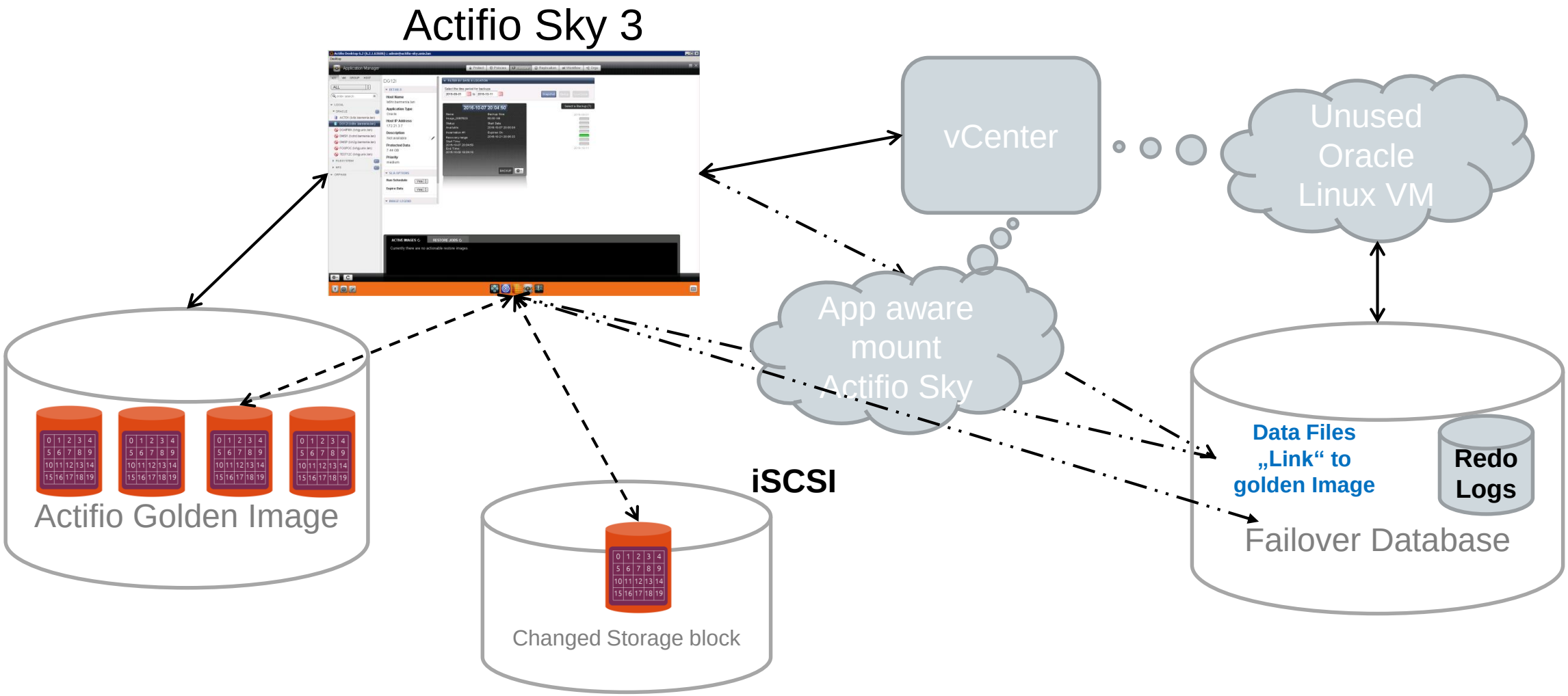
Sicherung einer Oracle Datenbank



Delta Sicherung auf Basis geänderter Storage Blöcke

Barmenia Versicherungen

Einsatz einer actifio backup Version bei Verlust der Original DB



Ist eine mit actifio gesicherte DB nicht nutzbar, kann man den Backup Storage von actifio für die Produktion nutzen. Die actifio Sky verwaltet dann die Änderungen auf dem Backup in Form von Snapshots.

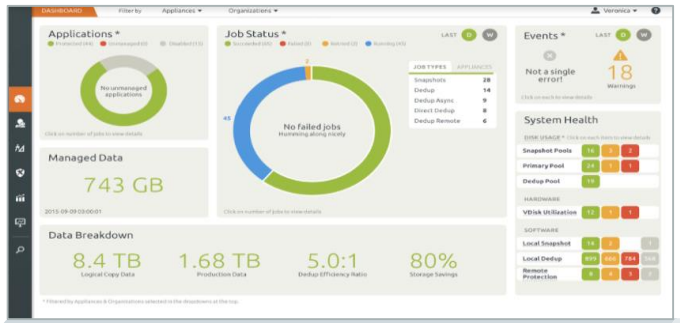
Barmenia Versicherungen

Die Building Pipeline mit Actifio verbinden

PRODUCTION APPLICATIONS

APP, DATABASE, & HYPERVISOR HOST SERVERS

Efficient, Incremental Data Capture

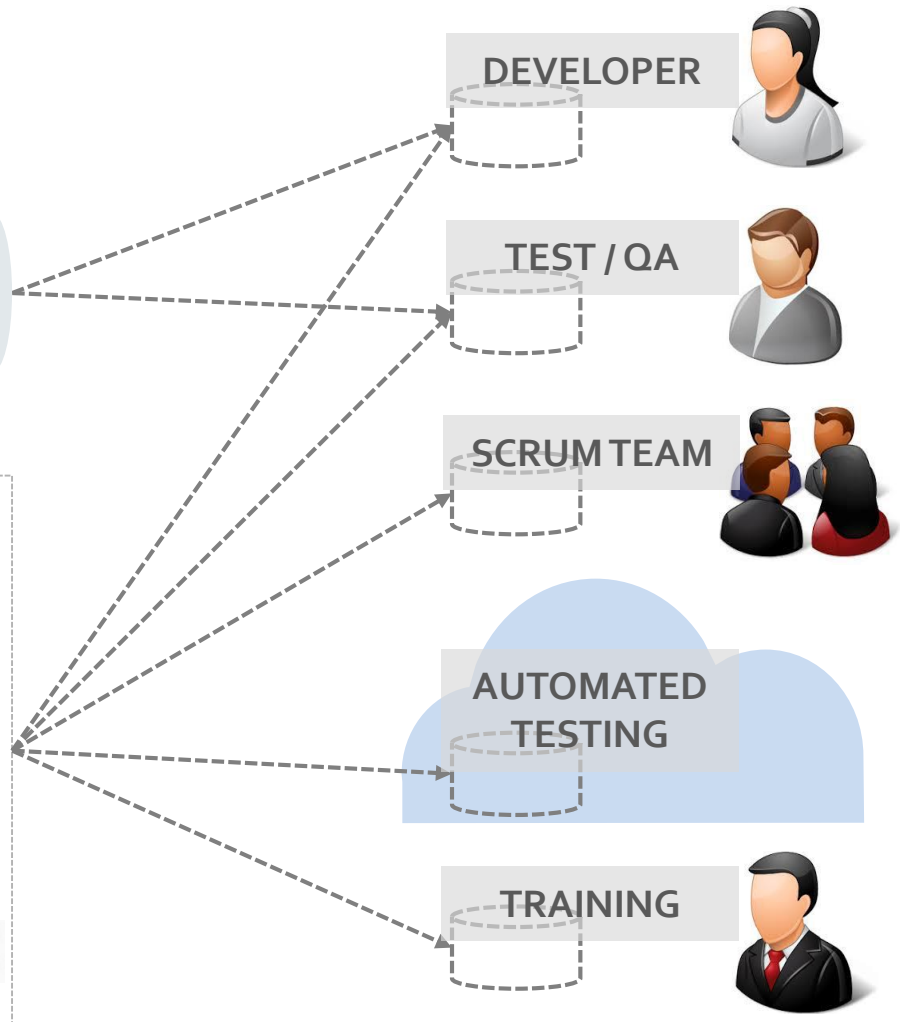


actifio *Virtual Data Pipeline*

API

Jenkins
CHEF
git
puppet
SALTSTACK
ANSIBLE
Maven
CAMOUFLAGE

DEVELOPMENT DATA USERS



COPYRIGHT 2015 ACTIFIO

Barmenia72 Versicherungen

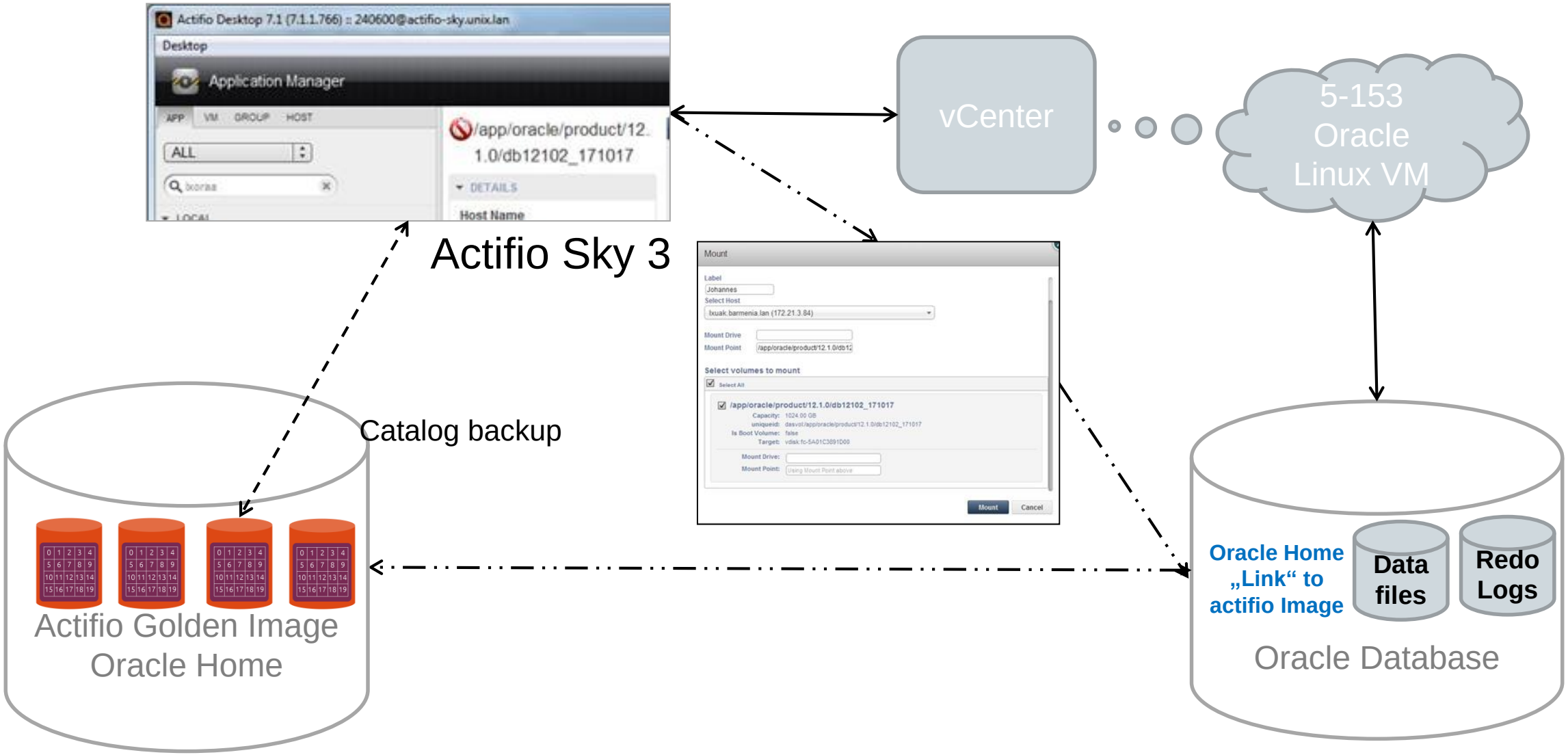
Viele Datenbanken mit nur 1 Oracle Home fahren

- Wir haben derzeit 186 Oracle Datenbanken
  - Unterteilt in die SLA "Basic", "Important" and "Critical"
- Ein Oracle Home benötigt ca. 7,3 GB Storage
- Wenn ein Patch ansteht muss ein neues Oracle Home auf alle VMs ausgerollt werden
- Der Status Quo der derzeit eingesetzten Oracle Homes sieht wie folgt aus:

Version	Release	Patch Number	Patch Description	Anzahl Release	Anzahl Patch Number
12.1.0.2.0	12.1.0.2.161018	24006101	Database Patch Set Update : 12.1.0.2.161018 (24006101)	6	6
12.1.0.2.0	-	26925311	DATABASE PATCH SET UPDATE 12.1.0.2.180116	0	5
12.1.0.2.0	12.1.0.2.171017	26713565	DATABASE PATCH SET UPDATE 12.1.0.2.171017	153	153

COPYRIGHT 2015 ACTIFIO

Viele Datenbanken mit nur 1 Oracle Home fahren



Barmenia Versicherungen

Die „versiegelte“ Cloud

Was macht die Sealed Cloud so einzigartig?

1. Die bereits in der EU und in den USA patentierte Sealed Cloud Technologie bietet die Vorteile einer Public Cloud kombiniert mit der Sicherheit einer Private Cloud.
2. Höchstes Sicherheitsniveau auch gegen Angriffe von innen durch die „Versiegelung“ der Cloud-Plattform
3. Anders als bei anderen Cloud-Lösungen hat niemand, auch nicht der Betreiber der Cloud, Datenzugriff.

Sealed Cloud – einzigartig sicher:
Nur der Eigentümer der Daten und von ihm explizit bestimmte Personen haben Zugriff auf die Daten

- Alle Applikationsserver befinden sich in elektromechanisch versiegelten Rack-Systemen.
- Die Server beinhalten nur flüchtige Speicher.
- Bevor ein Mitarbeiter oder Angreifer an die Server gelangt, werden alle unverschlüsselten Daten gelöscht.
- Das verwendete Betriebssystem ist zusätzlich gehärtet und sperrt alle externen Zugänge.
- Das System meldet zwar Statusinformationen nach außen, akzeptiert jedoch keine Befehle von außen.

Eine Kombination vieler Maßnahmen stellt sicher, dass im Datenzentrum kein Zugriff auf unverschlüsselte Daten erfolgen kann.

Die Sealed-Cloud-Technologie schafft mittels Versiegelung ein vertrauenswürdiges Daten-zentrum und ermöglicht so wesentlich höhere Sicherheit für Anwendungen und Daten.

Ein Whitepaper mit ausführlicheren Informationen finden Sie unter www.sealedcloud.de

Wie kann Compliance mehr Chance als nur Kosten sein?

- Innovationen und proaktives Handeln ist zwingend um am Markt zu bestehen.
  - Jede IT steht letztlich auch in Konkurrenz zu amazon, google, azure ….
- Revisionssicherheit ist im Kontext der EU Datenschutzregelung (DSGVO) noch bedeutsamer als heute, aber…
  - ohne Standards und Automation, ist kein kostengünstiger RZ Betrieb möglich und
  - mehr als „state of the art“ verlangt Compliance auch nicht.
- Es werden ständig neue Tools und Techniken auf dem Markt kommen.
  - Durch eigene Standards und der Schaffung fehlender (Rest)API Schnittstellen, kann man auf Basis von CMDB Daten sukzessive automatisieren
- **Alle Veränderungsprozesse muss man intensiv managen!**

Warum soll das nicht gleichzeitig auch kostengünstig und von Nutzen sein?

Fragen & Antworten

„AUF EINER SKALA VON 1-10: WIE VERWIRRT SIND SIE?“

„17.“

„NUR BIS 10.“

„WAS?“

„DIE SKALA.“

„WELCHE?“

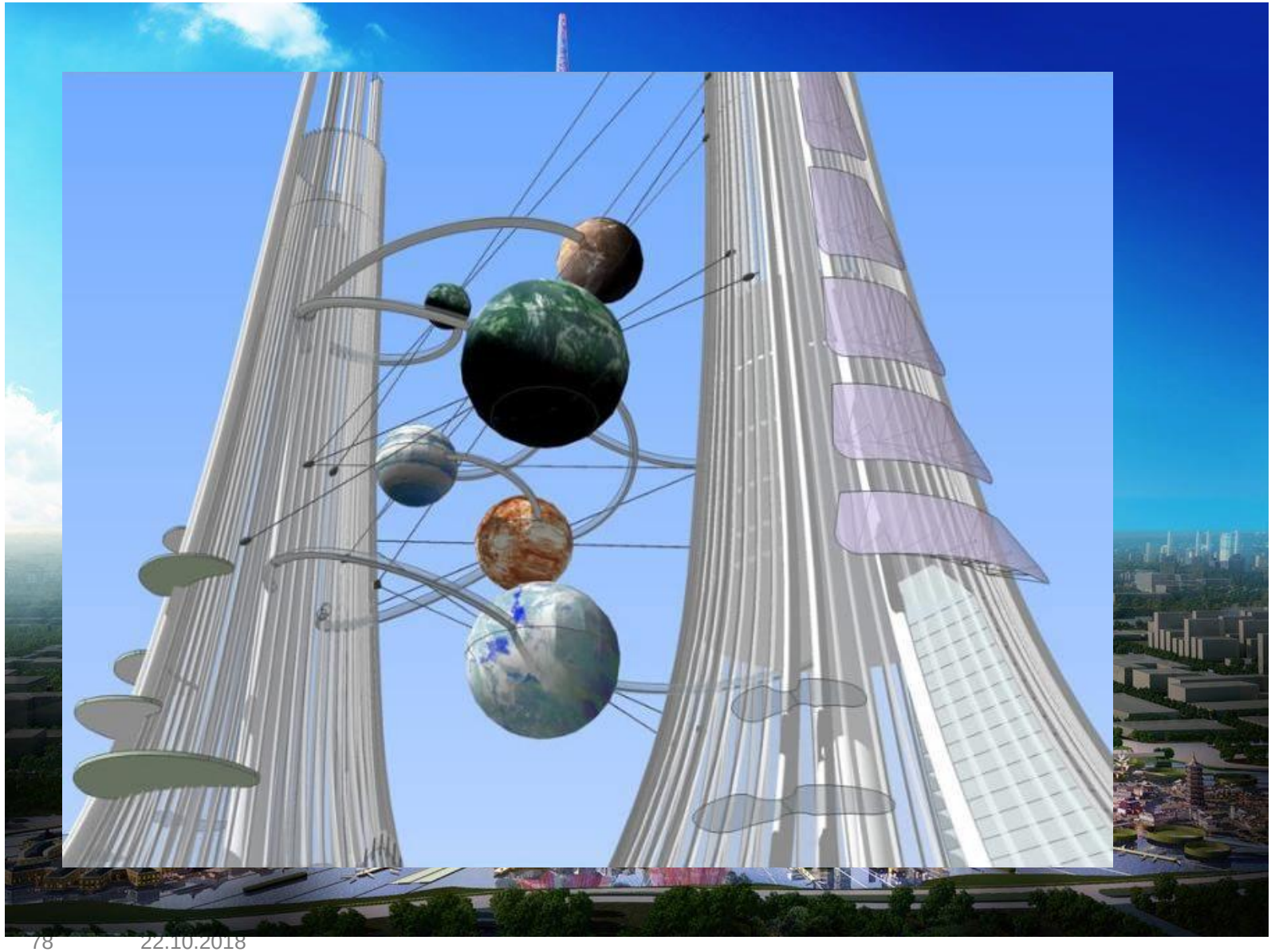
„WIE VERWIRRT SIE SIND!“

„ACHSO...17.“

DEBESTE

Barmenia Versicherungen

Unsere Träume können wir erst dann verwirklichen, wenn wir uns dazu entschließen daraus aufzuwachen. (Josephine Baker)



China plant in Wuhan Wolkenkratzer mit 1.000 Metern Höhe, die mit Skywalks verbunden werden sollen.
Warum immer wieder runter fahren, wenn man einfach auf 400 Metern „rüber“ gehen kann?!

Barmenia Versicherungen

Vielen Dank für Ihre Aufmerksamkeit!

Besser Barmenia. Besser leben.

Andre Lünsmann
Email: andre.luensmann@barmenia.de

Barmenia Versicherungen