DOAG 2015 Business Solutions Konferenz

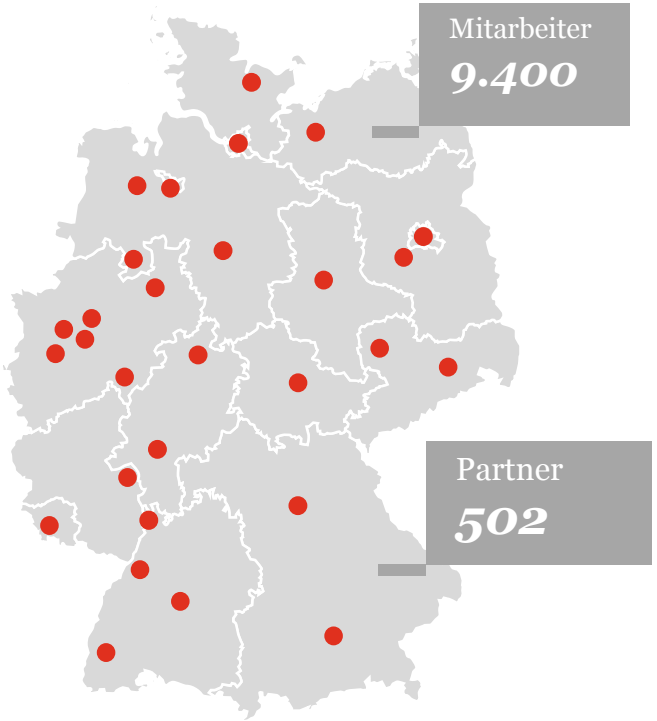
GoB bei Auslagerung
IDW ERS FAIT 5

Darmstadt, 09. Juni 2015

Timo Gröf
PwC Frankfurt
Risk Assurance Solutions

PwC in Deutschland

Mittelstands-Unternehmen
15.120



Mitarbeiter
9.400

Partner
502

29 Standorte

Berlin	Hamburg	Nürnberg
Bielefeld	Hannover	Oldenburg
Bremen	Karlsruhe	Osnabrück
Dresden	Kassel	Potsdam
Duisburg	Kiel	Saarbrücken
Düsseldorf	Köln	Schwerin
Erfurt	Leipzig	Siegen
Essen	Magdeburg	Stuttgart
Frankfurt/Main	Mainz	München
Freiburg	Mannheim	

Mandanten in Deutschland
37.350

pwc

Agenda

01 Anforderungen der Kunden an einen Cloud Provider auf Basis unserer aktuellen Studie

02 Welche Standards / Zertifizierungen gibt es? Welchen Nutzen stiften sie?

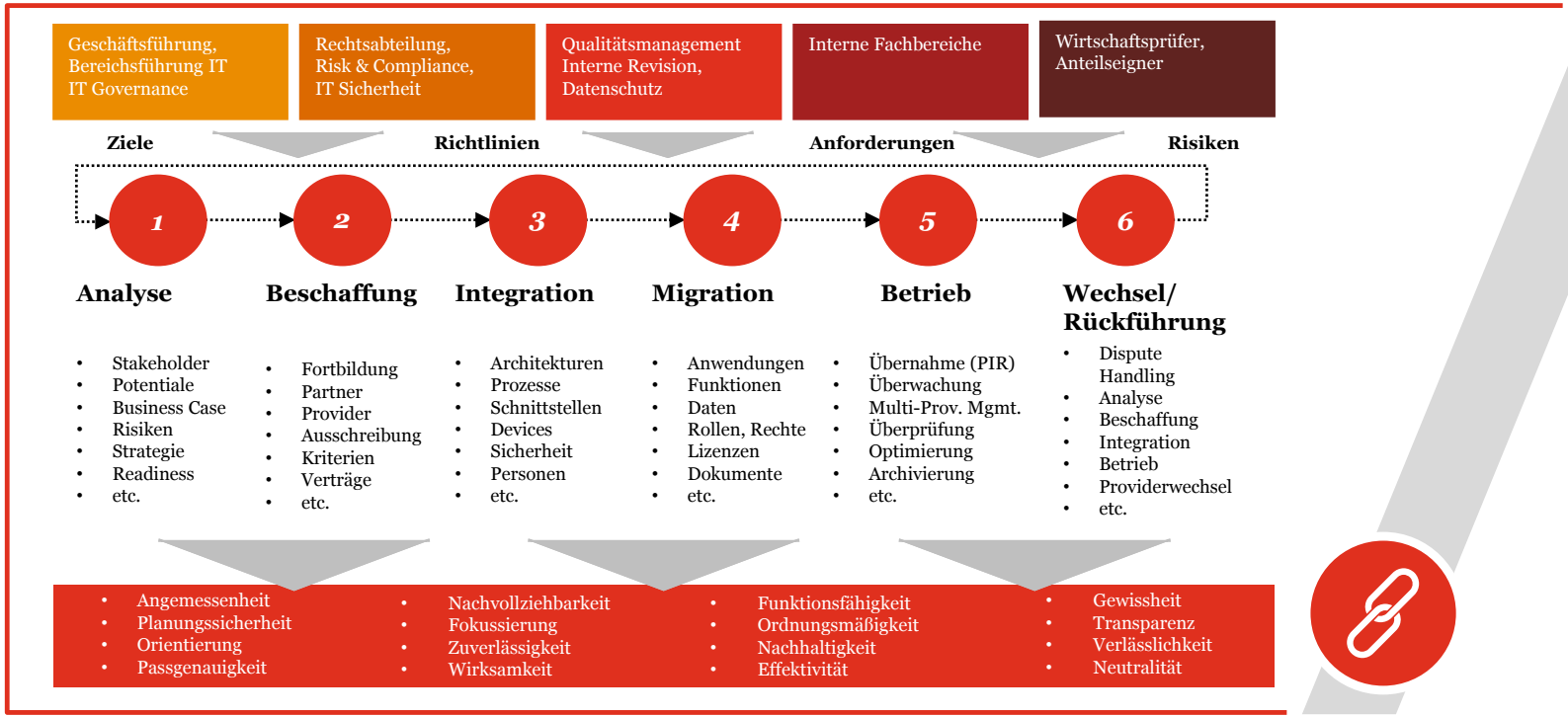
03 GoB bei Auslagerung nach IDW ERS FAIT 5

04 Wohin geht die Reise (Audit of the Future)?

05 Diskussion mit dem Plenum

Anforderungen der Kunden an einen Cloud Provider

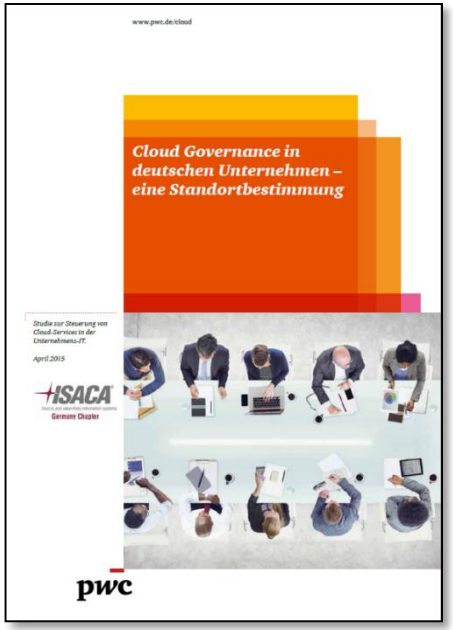
Anforderungen der Stakeholder in den Phasen eines Cloud Services



01

Anforderungen der Kunden an einen Cloud Provider

Aktuelle Studie zur Cloud Governance in deutschen Unternehmen



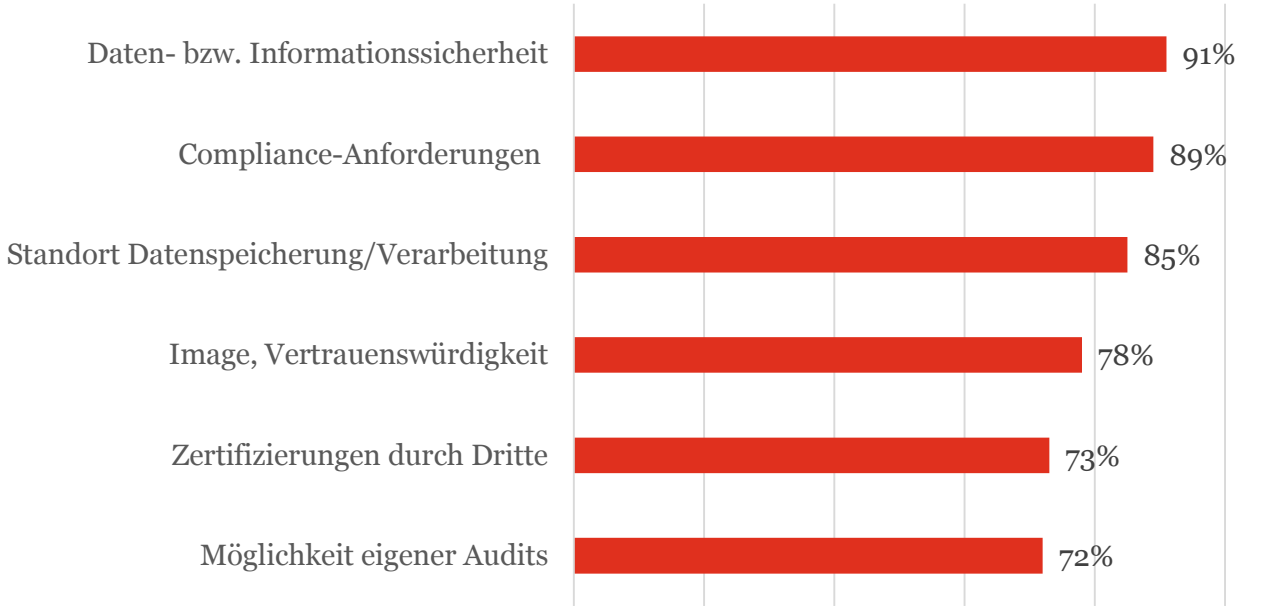
ISACA® Trust in, and value from, information systems Germany Chapter

pwc

- Antworten von 306 Mitgliedern des ISACA Germany Chapters
- Führungs- und Fachkräfte aus den Bereichen Finanzen, Revision, Audit, IT und Risikomanagement
- Deutscher Mittelstand als auch global agierende Konzerne

Anforderungen der Kunden an einen Cloud Provider

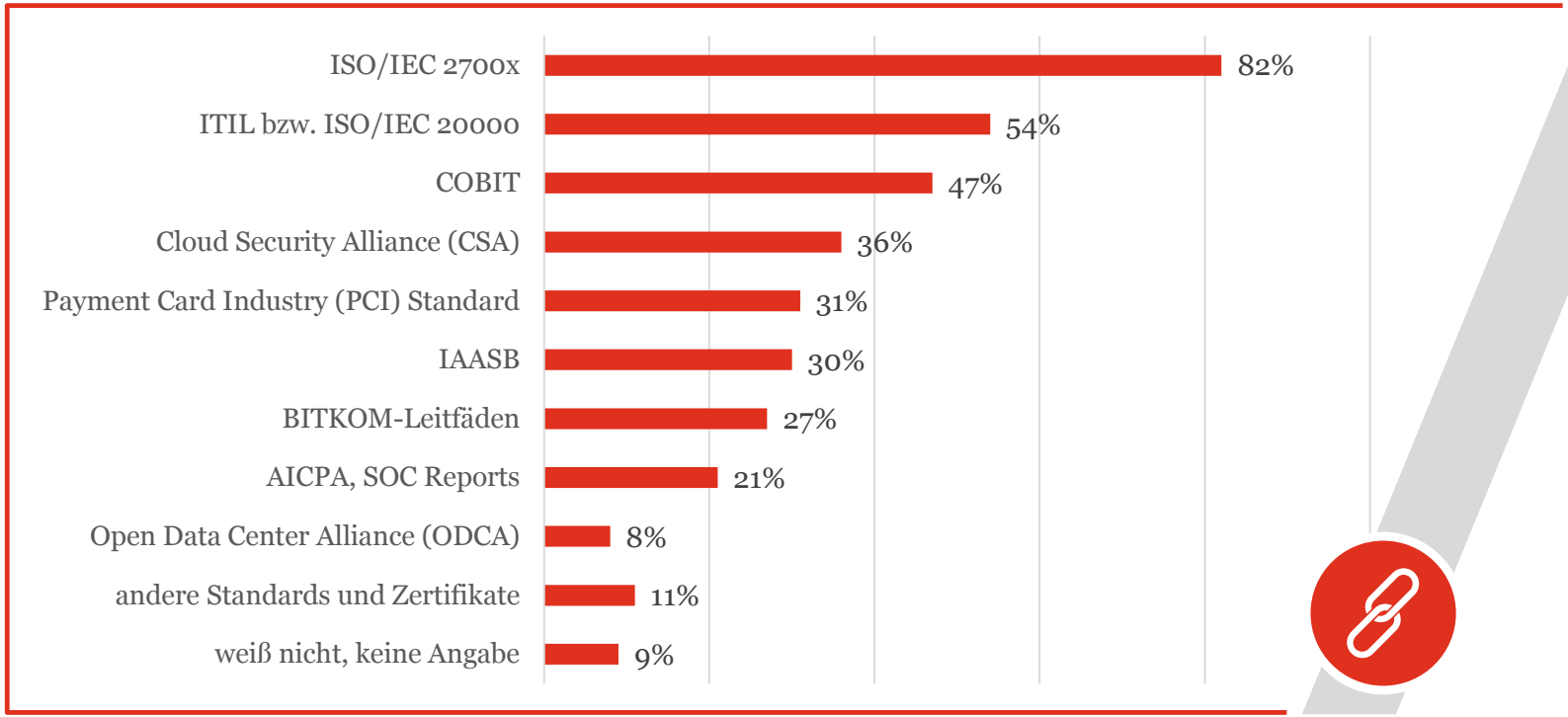
Bedeutung von Kriterien bei der Auswahl von Cloud Services und Cloud Providern



n = 306; Darstellung Anteile für Wertpunkte 10-7 "eher wichtig" auf der 10er-Skala

Anforderungen der Kunden an einen Cloud Provider

Relevante Standards und Zertifikate bei der Auswahl von Cloud Providern



Welche Standards / Zertifizierungen gibt es?

02

- **IDW ERS FAIT 5,**
  eine Brücke zwischen den IDW-Standards
- **CSA STAR Certification/Attestation,**
  im Cloud-Umfeld bekannt, aber noch nicht verbreitet
- **AICPA Trust Services Principles Criteria (SOC 2),**
  bekannt und verbreitet bei Providern in Nordamerika
- **IDW RS FAIT 1 & PS 330,**
  Kriterien des Wirtschaftsprüfers in der Jahresabschlussprüfung
- **IDW PS 951/ISAE 3402/SSAE16,**
  Bescheinigung über die Kontrollen eines Dienstleisters
- **ISO/IEC 27001:203,**
  der Klassiker zur Zertifizierung eines ISMS

GoB bei Auslagerung/Cloud Computing

IDW ERS FAIT 5 – Hintergrund

- Entwurf einer IDW **Stellungnahme zur Rechnungslegung**: *„Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud Computing“*
- Entwickelt in einer Arbeitsgruppe des IDW unter maßgeblicher Beteiligung von Experten der „Big 4“ (Deloitte, EY, KPMG, PwC)
- Im November 2014 auf der Website des IDW veröffentlicht, um dem Berufsstand und der interessierten Öffentlichkeit die Möglichkeit der Kenntnis- und Stellungnahme zu bieten.
  → dies ist noch bis 30. Juni möglich.

GoB bei Auslagerung/Cloud Computing

IDW ERS FAIT 5 zu Sicherheits- und Ordnungsmäßigkeitsanforderungen

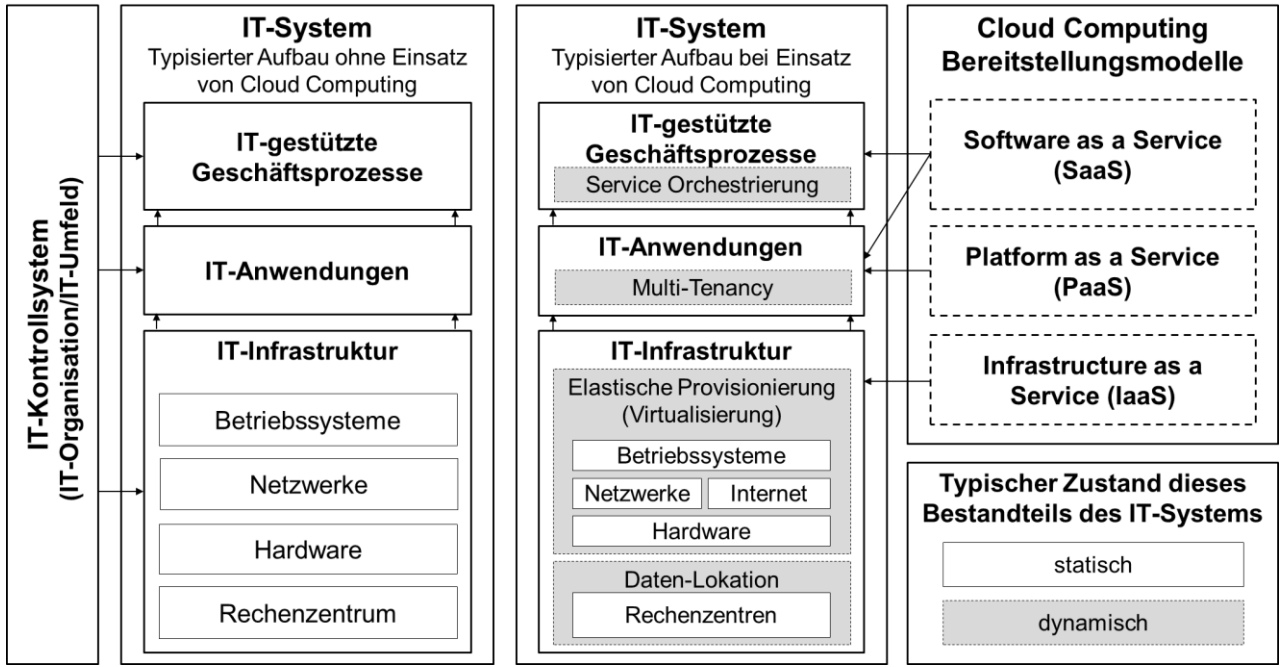
Die GoB (§§ 238, 239 HGB) und die damit verbundenen Anforderungen an die Sicherheit der IT-gestützten Rechnungslegung gelten uneingeschränkt und haben sich durch Cloud Computing nicht geändert.

Grundsatz	Anforderung gemäß	i.d.R. unterstützt durch
Vollständigkeit	§ 239 Abs. 2 HGB	Journalfunktion
Richtigkeit	§ 239 Abs. 2 HGB	Belegfunktion, Kontenfunktion
Zeitgerechtheit	§ 239 Abs. 2 HGB	Journalfunktion
Ordnung	§ 239 Abs. 2 HGB	Kontenfunktion
Nachvollziehbarkeit	§ 238 Abs. 1 HGB	Belegfunktion, Verfahrensdokumentation
Unveränderlichkeit	§ 239 Abs. 3 HGB	Belegfunktion

- ***Voraussetzung für die Ordnungsmäßigkeit ist die Sicherheit!***
- *Maßnahmen zum Gewährleisten der **Vertraulichkeit, Integrität, Verfügbarkeit, Autorisierung, Authentizität und Verbindlichkeit** müssen sachgerecht implementiert und kontinuierlich wirksam sein.*

GoB bei Auslagerung/Cloud Computing

IDW ERS FAIT 5 – Typsicher Aufbau eines IT-Systems in der „alten“ und „neuen“ Welt



GoB bei Auslagerung/Cloud Computing

IDW ERS FAIT 5 – Beispielhafte Sicherheitsanforderungen

Ebene	Beispielhafte Sicherheitsanforderungen
IT-Kontroll-umfeld & IT-Organisation	**Anpassen der Sicherheitskonzepte** in Bezug auf die Adressierung Technologie-spezifischer Risiken – **Klassifizierung von Daten** im Zusammenhang mit dem Bereitstellungsmodell und der Datenlokation – **Verschlüsselung der Daten** während Übertragung und Speicherung durch geeignete kryptographische Verfahren
IT-Infrastruktur	• Vollständige und nachvollziehbare **Dokumentation der Verfahren** für den geordneten Regelbetrieb als auch für den Notfallbetrieb • Regelmäßige Überprüfung der zuverlässigen **Trennung** von vertrauenswürdigen und nicht vertrauenswürdigen **Netzwerken** (z.B. Berichte nach ISAE 3402)
IT-Anwendung	• Bescheinigung über die **Angemessenheit** der anwendungsbezogenen, **automatischen Kontrollen** (z.B. Berichterstattung nach IDW PS 880) • Angemessenes **Softwareentwicklungs- und Programmänderungs-verfahren**, z.B. durch Tool-Unterstützung in Entwicklung, Test und Freigabe
IT-gestützte Geschäfts-prozesse	• **Regelungen** für das **Format**, in dem **Daten** an den Dienstleister übergeben und wieder übergeleitet werden • **Schnittstellenkontrollen**, inkl. Prüfung auf Vollständigkeit, Plausibilität oder rechnerische Richtigkeit (soweit individualisierbar)

Wohin geht die Reise?

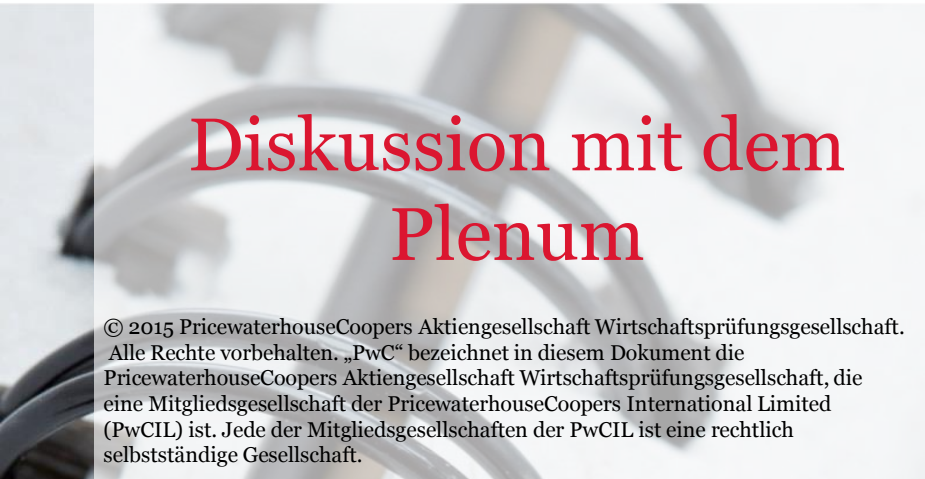
Audit of the Future

- Cloud Nutzer: Fordern “Report on Demand”
- Manuelle Prüfungshandlungen werden der Vergangenheit angehören.
- Vielmehr werden automatisierte Kontrollen und Datenanalysen Nachweise liefern.
- Dann werden Cloud Services nicht mehrmals im Jahr zertifiziert sondern einmal
  - Systembeschreibung /Konzept
  - Funktionalitäten
  - Compliance Transformation und Customizing

Diese Entwicklung begleiten wir heute schon bei PwC.

Vielen Dank für Ihre Aufmerksamkeit

DOAG 2015 Business Solutions Konferenz



Diskussion mit dem Plenum