

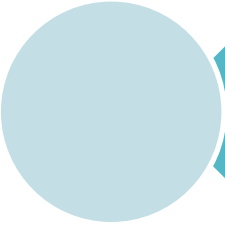
Anforderungen an IT-Sicherheit bei Banken

Jochen Kindermann
Partner

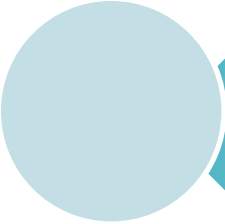
26. April 2018



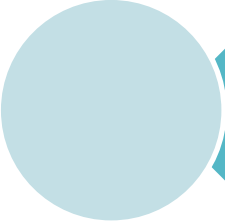
Agenda



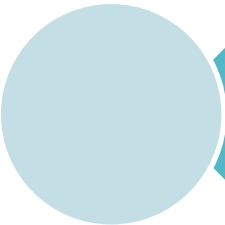
Stand der Regulierung



Regulatorische Anforderungen nach MaRisk / BAIT

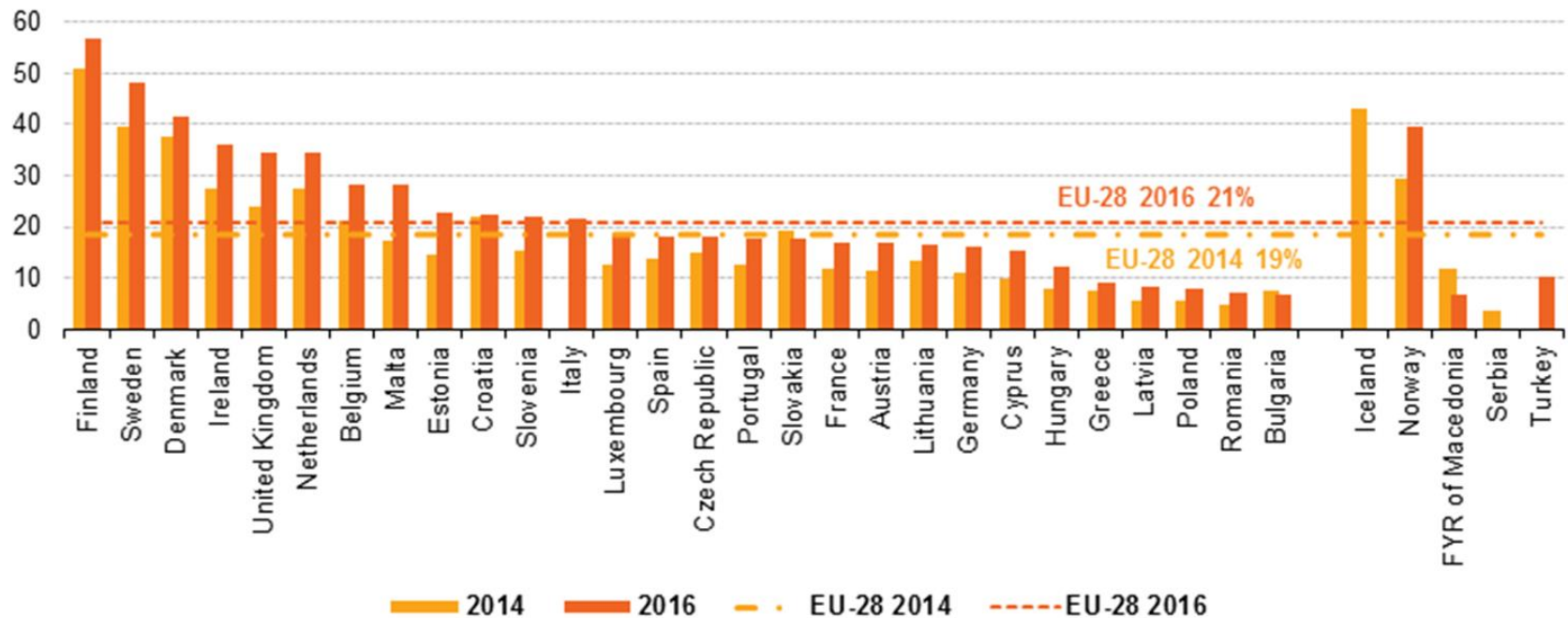


Regulierung auf europäischer Ebene – EBA-Leitlinien



Regulierung des Cloud Computing - Quo vadis?

Statistik – Nutzung von Cloud Computing in Europa



Italy: break in series; Iceland, Serbia: 2016 not available; Turkey: 2014 not available

Statistik bzgl. der Cloudnutzung von Unternehmen in Europa
(2014/2016); Quelle: Eurostat

Übersicht – Regulierung



Regelwerk um Cloud Services

Stand der Regulierung - International

Verlautbarungen europäischer Aufsichtsbehörden

- Circular CSSF 17/654 (Luxemburg, 2017)
- Guidelines FCA (Großbritannien, 2016)
- Rundschreiben 2018/3 der FINMA (Schweiz, 2018)

EBA-Leitlinien

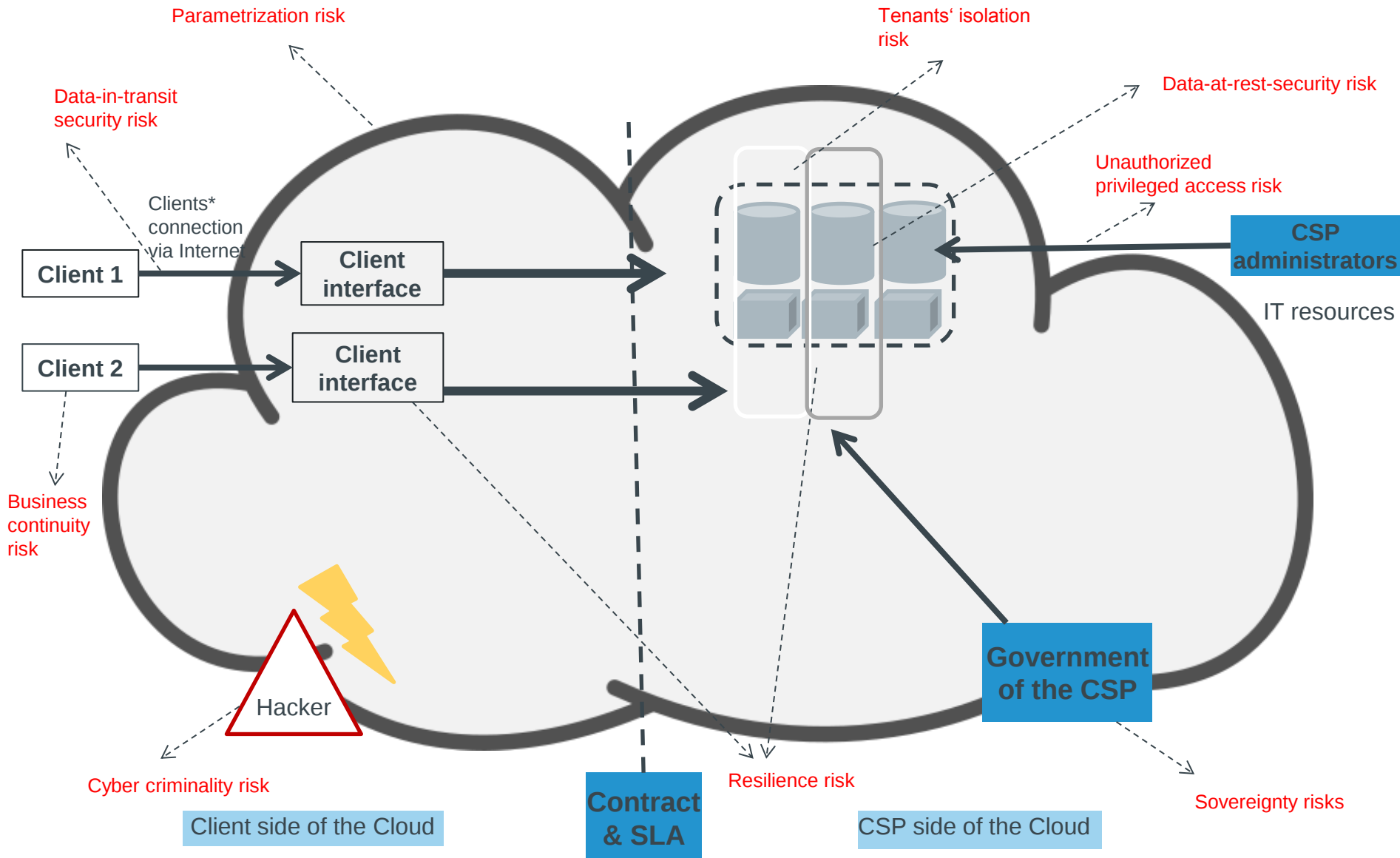
- Recommendations on outsourcing to cloud services providers (EU, 2017)

Deutschland

- BaFin: Orientierungshilfe Cloud-Auslagerung (geplant)



Risiken der Auslagerung in die Cloud



Regulatorische Anforderungen – MaRisk

MaRisk AT 9

Einordnung

- Konkretisierung § 25a / 25b KWG i.V.m. den MaRisk Vorgaben

Inhalte

- Abgrenzung auslagerbare / nicht auslagerbare Aktivitäten und Prozesse
- „Wesentlichkeit“
- Verantwortung verbleibt bei der Geschäftsleitung; Leitungsaufgaben sind nicht auslagerbar
- Anforderungen an Auslagerungsverträge
- Kontinuität und Qualität der ausgelagerten Aktivitäten und Prozesse
- Steuerung und Überwachung der Risiken
- Informations- und Prüfrechte sowie Kontrollmöglichkeiten der BaFin
- Regelungen mit dem Umgang von Weiterverlagerungen (Kettenverlagerungen) müssen vorhanden sein

Gegenstand des Auslagerungsvertrages

- a) Spezifizierung und ggf. Abgrenzung der vom Auslagerungsunternehmen zu erbringenden Leistung
- b) Festlegung angemessener Informations- und Prüfungsrechte der Internen Revision sowie externer Prüfer
- c) Sicherstellung der uneingeschränkten Informations- und Prüfungsrechte sowie der Kontrollmöglichkeiten der gemäß § 25b Absatz 3 KWG zuständigen Behörden bezüglich der ausgelagerten Aktivitäten und Prozesse
- d) soweit erforderlich Weisungsrechte
- e) Regelungen, die sicherstellen, dass datenschutzrechtliche Bestimmungen und sonstige Sicherheitsanforderungen beachtet werden
- f) Kündigungsrechte und angemessene Kündigungsfristen
- g) Regelungen über die Möglichkeit und über die Modalitäten einer Weiterverlagerung, die sicherstellen, dass das Institut die bankaufsichtsrechtlichen Anforderungen weiterhin einhält
- h) Verpflichtung des Auslagerungsunternehmens, das Institut über Entwicklungen zu informieren, die die ordnungsgemäße Erledigung der ausgelagerten Aktivitäten und Prozesse beeinträchtigen können

Regulierung auf Europäischer Ebene

Schwerpunkte der EBA-Empfehlungen

- Wesentlichkeit
- Informationspflichten
- Zugangsrechte
- Weisungsrechte
- Audit Rechte
- Lokation der Daten
- Kettenauslagerung
- Datensicherheit /-schutz



Wesentlichkeit

Risikoanalyse – Kriterienkatalog

- Kritikalität und Risikoprofil der auszulagernden Dienstleistung; d.h. Beurteilung, ob diese Tätigkeiten zur Aufrechterhaltung des Geschäftsbetriebs/Existenzfähigkeit des Instituts und seiner Verpflichtungen gegenüber Kunden kritisch ist
- Unmittelbare operative Auswirkungen von Ausfällen und damit verbundene Rechts- und Reputationsrisiken
- Auswirkungen einer Unterbrechung der Geschäftstätigkeit für die Ertragsentwicklung des Instituts
- Potentielle Folgen einer Vertraulichkeitsverletzung oder eines Versagens der Datenintegrität für das Institut oder seine Kunden

Zugangs- und Prüfrechte (1)

- Umfassendes Zugangsrecht:
„including the full range of devices, systems, networks and data used in providing the services“
- Unbegrenzttes Recht zu Inspektion und Kontrolle (Audit) in Bezug auf die ausgelagerte Dienstleistung
- Aber: risikobasierter Ansatz:
 - Pooled audit
 - Auditorbestätigung + Auditreport des Dienstleisters



Zugangs- und Prüfungsrechte (2)

Auditreport des Dienstleisters

- Prüfungsbericht muss Systeme und Kontrollen umfassen
 - Berichte sind laufend auszuwerten
 - Qualifikation der Prüfer ist zu überwachen
 - Prüfungen sind anhand anerkannter Prüfungsstandards sicherzustellen
 - Recht zur Ausweitung der Prüfung ist vorzusehen:
„number and frequency should be reasonable and legitimate“



Datenlokation und Datenverarbeitung

Hohe Anforderungen bei Auslagerungen außerhalb des EWR

Risikobasierter Ansatz unter Berücksichtigung von

- Rechtsrisiken
- Compliancerisiken
- Mangelnde Weisungsmöglichkeiten
- Politische Risiken
- Stabilitätsrisiken
- Durchsetzbarkeit eigener Maßnahmen
- Insolvenzrisiko
- Datenschutz im Zielland

Drittlandaus-
lagerung

Q&A



Jochen Kindermann
Partner, Frankfurt

T +49 69 9074 5443
jochen.kindermann@simmons-simmons.com