BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Konferenz „IT-Aufsicht bei Banken“

Ira Steinbrecher, Referatsleiterin
Referat GIT 3
Grundsatz IT-Aufsicht und
Prüfungswesen

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

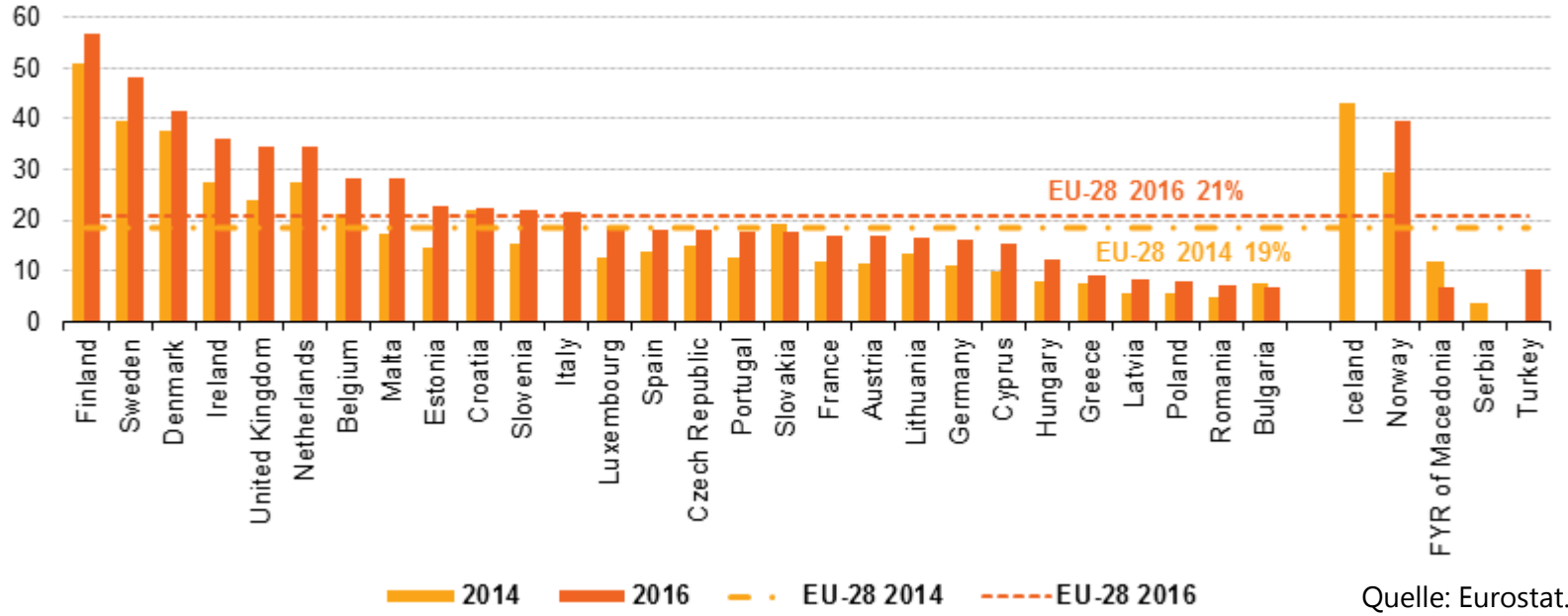
Cloud-Computing

IT-Aufsicht bei Banken am 27.09.2018

Inhalt

1.1 Überblick

- Auslagerungen europäischer und deutscher Unternehmen in die „Cloud“ nehmen zu:

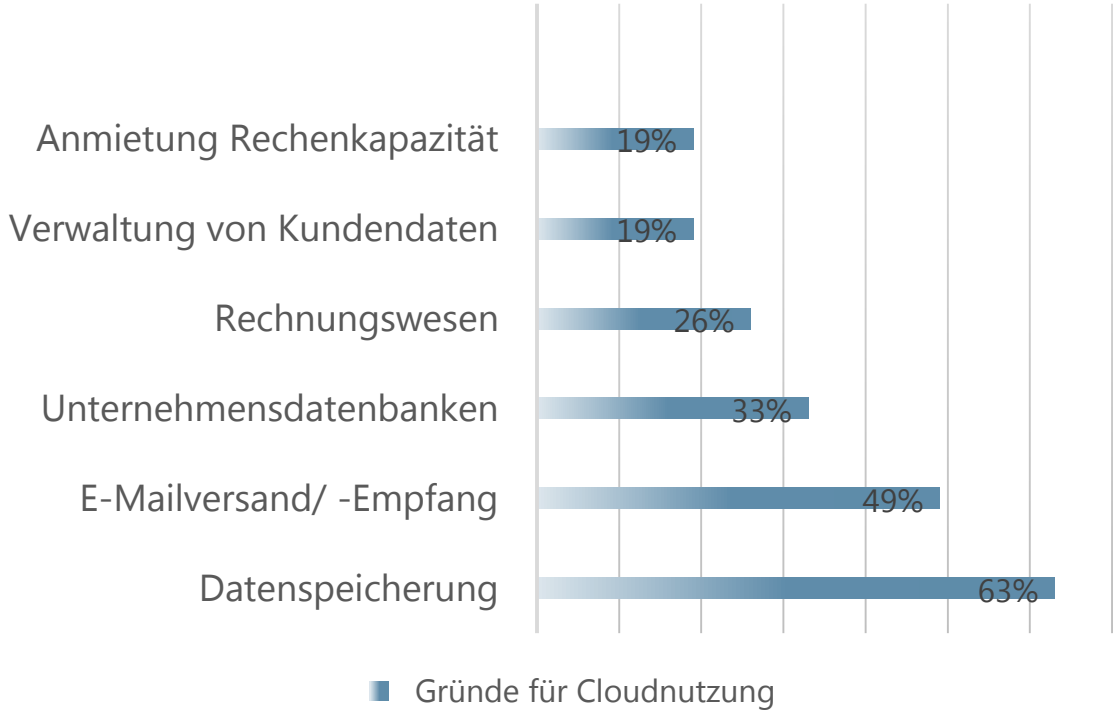


Quelle: Eurostat.

- Deutsche Unternehmen 2014: ca. 12 %; 2016: ca. 17 %
- 2016 nutzten ca. 59% der deutschen Banken und ca. 58% der deutschen Versicherungen Cloud-Angebote.

1.1 Überblick

- Deutsche Unternehmen haben Cloud-Dienste im Jahr 2016 aus folgenden Gründen genutzt :



Quelle: Statistisches Bundesamt.

1.2 Kriterien für Cloudnutzung

- Wichtige Kriterien deutscher Unternehmen bei der Auswahl des Cloud-Anbieters:
  - Konformität mit der seit Mai 2018 geltenden DSGVO (97 %)
  - transparente Sicherheitsarchitektur und -kontrollen (83 %)
  - die Ausstiegsstrategie (Exit) im Vertrag regelbar (79 %)
  - Hauptsitz im Rechtsgebiet der EU (76 %)
  - Integrationsfähigkeit der Lösungen (72 %)
  - Mögliche Datenverschlüsselung durch Cloudnutzer (71 %)
  - Unabhängige Zertifikate (70 %)
  - Rechenzentren im EU Rechtsgebiet (69 %)

Quelle: KPMG Cloud-Monitor 2018, Seite 13.

Inhalt

2.1 Internationale Ebene

- G7 ➔ Entwicklung der G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector ➔ bauen insbesondere auf den G-7 Fundamental Elements of Cybersecurity for the Financial Sector (veröffentlicht im Oktober 2016) auf:
  - Veröffentlichung 2018, Elemente sind nicht verbindlich.
  - Elemente sollen einen einheitlichen Rahmen im Umgang mit Cyberrisken vorgeben, die im Zusammenhang mit der Wahrnehmung von Aufgaben durch Dritte (z.B. Auslagerung) stehen.
  - Elemente behandeln insbesondere den Bereich Governance, den Umgang mit Cyberrisken, insbesondere deren Abbildung im Risikomanagement sowie Empfehlungen zur Vertragsgestaltung.
  - Elemente sollen insbesondere von beaufsichtigten Unternehmen berücksichtigt werden.

2.1 Europäische Ebene

- FinTech-Aktionsplan der Europäischen Kommission vom 08. März 2018:
  - Neben der EBA beschäftigen sich auch ESMA und EIOPA mit den Anforderungen bei der Nutzung von Cloud-Diensten.
  - Entwicklung von Standardvertragsklauseln für die Inanspruchnahme von Cloud-Diensten durch Finanzinstitute wird von der Europäischen Kommission befürwortet und gefördert.
  - Einrichtung eines EU-FinTech-Labs, um Kompetenzen und Wissen der Regulierungs- und Aufsichtsbehörden im Bereich der neuen Technologien zu verbessern.

Hinweis:
Einführung technologischer Innovationen im Finanzsektor soll damit gefördert werden.

2.2 Europäische Ebene

- EBA „Recommendations on outsourcing to cloud service providers“ (EBA/REC/2017/03 vom 20. Dezember 2017):
  - Integration in die Überarbeitung der EBA GL on Outsourcing (öffentliche Konsultation bis 24.09.2018)
  - Inhalte der seit Juli 2018 geltenden Recommendations sind u.a.:
    - Beurteilung der Wesentlichkeit
    - Informationspflichten gegenüber der Aufsicht und Prüfungsrechte für Banken und die Aufsicht
    - Geographische Lage der Daten bzw. Datenverarbeitung
    - Weiterverlagerungen sowie Ausstiegsklauseln

Hinweis:
Schaffung eines einheitlichen europäischen Rahmens im Umgang mit Auslagerungen an Cloud-Anbieter.

Inhalt

3.1 Inhalte

Hintergrund

- BaFin und Deutsche Bundesbank teilen ihre aufsichtliche Einschätzung zur Auslagerung an Cloud-Anbieter und der Einhaltung der damit verbundenen aufsichtsrechtlichen Anforderungen mit.
- Zweck: Die Orientierungshilfe stellt die aufsichtsrechtlichen Anforderungen an Auslagerungen von IT-Dienstleistungen im Lichte der Nutzung von Cloud-Diensten dar.
- Bestehende Anforderungen an Auslagerungen bleiben unberührt.

  ➔ Es werden keine neuen Anforderungen formuliert!

3.1 Inhalte

Adressaten:

- Beaufsichtigte Unternehmen ➔ Banken, Versicherungen
- Information für Cloud-Anbieter

Definitionen:

- Definition von Cloud-Diensten

  ➔ Übernahme der Definition der EBA

Definition der European Banking Authority (EBA):

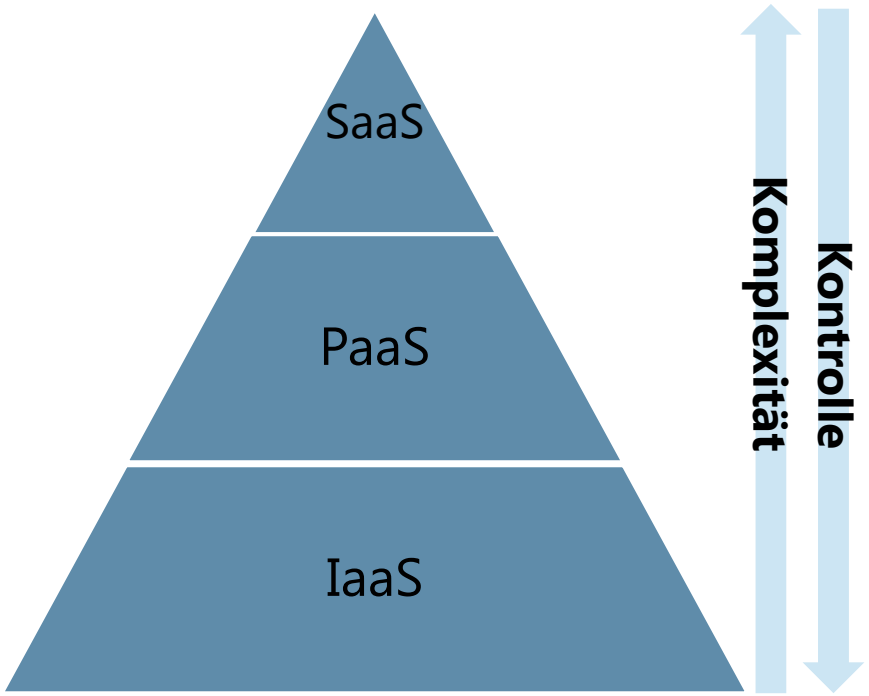
Cloud-Dienste: Dienste, die mithilfe von Cloud-Computing erbracht werden, d.h. ein Modell, das ortsunabhängigen, komfortablen und bedarfsgesteuerten Netzwerkzugriff auf einen gemeinsamen Pool konfigurierbarer Rechenressourcen ermöglicht (wie Netzwerke, Server, Speicher, Anwendungen und Services) und sich schnell sowie mit einem Mindestmaß an Verwaltungsaufwand oder Interaktion des Dienstleisters implementieren und freischalten lässt.

Quelle: EBA recommendations on outsourcing to cloud service providers vom 20.12.2017.

3.1 Inhalte

Dienstleistungsmodelle:

- Software as a Service (SaaS) ➔ Sämtliche Angebote von Anwendungen, die den Kriterien des Cloud Computing entsprechen, fallen in diese Kategorie.
- Plattform as a Service (PaaS) ➔ Ein PaaS-Provider stellt eine komplette Infrastruktur bereit und bietet dem Kunden auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden.
- Infrastructure as a Service (IaaS) ➔ IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze werden als Dienst angeboten.



Quelle: vgl. https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html (zuletzt aufgerufen am 18.09.2018).

3.1 Inhalte

Bereitstellungsmodelle:

- Öffentliche Cloud ➔ Cloud-Infrastruktur, die von der Öffentlichkeit frei genutzt werden kann.
- Private Cloud ➔ Cloud-Infrastruktur, die ausschließlich von einem einzelnen Institut genutzt werden kann.
- Community Cloud ➔ Cloud-Infrastruktur, die ausschließlich von einer konkreten Institutsgemeinschaft genutzt werden kann, einschließlich mehrerer Institute innerhalb einer Gruppe.
- Hybrid Cloud ➔ Cloud-Infrastruktur, die sich aus zwei oder mehreren speziellen Cloud-Infrastrukturen zusammensetzt.

Quelle: vgl. EBA/REC/2017/03 vom 20.12.2017, Seite 3.

3.1 Inhalte

Analyse und Wesentlichkeitsbetrachung:

- Unternehmen, die die Nutzung eines Cloud-Dienstes beabsichtigen, müssen prüfen, inwieweit dabei die aufsichtsrechtlichen Anforderungen an Auslagerungen zu beachten sind. → Einzelfallprüfung erforderlich
- Maßgeblich für die Prüfung des Vorliegens einer Auslagerung ist, ob und welche Aktivitäten/Prozesse an den Cloud-Anbieter übertragen werden.
- (nicht abschließende) Aufzählung wesentlicher Inhalte der Risikoanalyse, z.B.:
  - Bewertung der Risiken, die sich aus dem gewählten Dienstleistungsmodell/ Bereitstellungsmodell ergeben können
  - Bewertung der Eignung des Cloud-Anbieters (Know-how, Infrastruktur , wirtschaftliche Situation, gesellschaftsrechtlicher und regulatorischer Status etc.)

Nutzung von Cloud-Diensten ist in der Regel eine Auslagerung

3.1 Inhalte

Anforderungen bei wesentlicher Auslagerung zur Vertragsgestaltung:

- **Leistungsgegenstand:** Spezifizierung und ggf. Abgrenzung der vom Cloud-Anbieter zu erbringenden Leistung (Service Level Agreements)

- **Rechte des beaufsichtigten Unternehmens:** Festlegung der Informations- und Prüfungsrechte, insbesondere Möglichkeit der Durchführung von Vor-Ort-Prüfungen
  - Keine Einschränkungen der Rechte, z.B. gestufte Informations-, Prüfverfahren, Prüfung wird von der wirtschaftlichen Zumutbarkeit (commercially reasonable) abhängig gemacht; alleiniger Verweis auf Zertifikate
  - Erleichterungen ➔ „Pool-Audits“, Durchführung von Prüfungen durch die Interne Revision des Cloud-Anbieters (BT 2.1 Tz. 3 MaRisk)

3.1 Inhalte

Anforderungen bei wesentlicher Auslagerung zur Vertragsgestaltung:

- **Rechte der Aufsicht**: Sicherstellung der uneingeschränkten Informations- und Prüfungsrechte sowie der Kontrollmöglichkeiten der Aufsicht bezüglich der ausgelagerten Aktivitäten und Prozesse, z.B.
  - Möglichkeit der Durchführung von Vor-Ort-Prüfungen
  - Überprüfung des ausgelagerten Sachverhalts muss beim Cloud-Anbieter ebenso möglich sein wie beim beaufsichtigten Unternehmen.

- **Weisungsrechte:** Sicherstellung, dass alle erforderlichen und zur Erfüllung der vereinbarten Dienstleistung notwendigen Weisungen erteilt werden können

3.1 Inhalte

Anforderungen bei wesentlicher Auslagerung zur Vertragsgestaltung:

- **Datensicherheit/-schutz:** Regelungen, die sicherstellen, dass datenschutzrechtliche Bestimmungen und sonstige Sicherheitsanforderungen eingehalten werden (Hinweis zum Ort der Datenspeicherung)

- **Kündigungsmodalitäten:** Kündigungsrechte und angemessene Kündigungsfristen (Sicherstellung der Aufrechterhaltung der Dienste, Rückübertragungsmodalitäten)

- **Weiterverlagerung/Subdelegation:** Regelungen über die Möglichkeit und über die Modalitäten einer Weiterverlagerung, die sicherstellen, dass die aufsichtsrechtlichen Anforderungen weiterhin eingehalten werden (ggf. Zustimmungserfordernis)

3.1 Inhalte

Anforderungen bei wesentlicher Auslagerung zur Vertragsgestaltung:

- **Informationspflichten:** Pflicht des Cloud-Anbieters, das beaufsichtigte Unternehmen über Entwicklungen zu informieren, die die ordnungsgemäße Erledigung der ausgelagerten Aktivitäten und Prozesse beeinträchtigen können

- **Weitere Themen:** Hinweis zum anwendbaren Recht

3.2 Ausblick

- Orientierungshilfe als „lebendes Dokument“ geplant ➔ Aktualisierungen erfolgen, wenn notwendig.

- BaFin und Deutsche Bundesbank werden auch zukünftige Entwicklungen bei Auslagerungen an Cloud-Dienstleister angemessen adressieren.

Vielen Dank für Ihr Interesse!

Ira Steinbrecher,
Referatsleiterin Referat GIT 3

Tel. +49 (0)228 / 4108-1075

Ira.Steinbrecher@bafin.de

Bankenaufsicht, Gruppe IT-Aufsicht
Grundsatz IT-Aufsicht und Prüfungswesen