DEUTSCHE BÖRSE GROUP

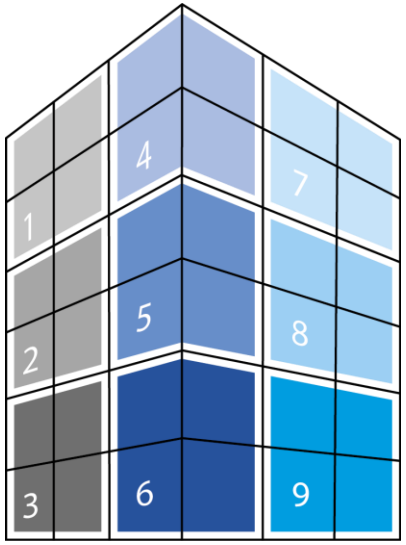
Collaborative Cloud Audit Group (CCAG)

Michael Girg, Chief Cloud Officer Deutsche Börse Group
Bastian Bahnemann, Executive Office IT, Deutsche Börse Group

26 APR 2018

An overview of Deutsche Börse Group

Deutsche Börse Group covers the entire value chain in securities and derivatives trading.



1 Pre-IPO and listing
2 Trading
3 Clearing

4 Settlement
5 Custody
6 Collateral and liquidity management

7 Market data
8 Indices
9 Technology

Cloud is part of any modern technology stack – financial industry strives for cloud adoption, too

- Cloud is part of any modern technology stack and a competitive element
- Cloud implementation in highly regulated financial industry is challenging - adaption within financial industry in Europe lacks behind
- Important business priority also for Deutsche Börse Group
- Group audit format was picked up in recent regulation
- Cloud audit group initiated in 2017 to enable cloud adaption by achieving outsourcing compliance
- Audit group designed as completely open format

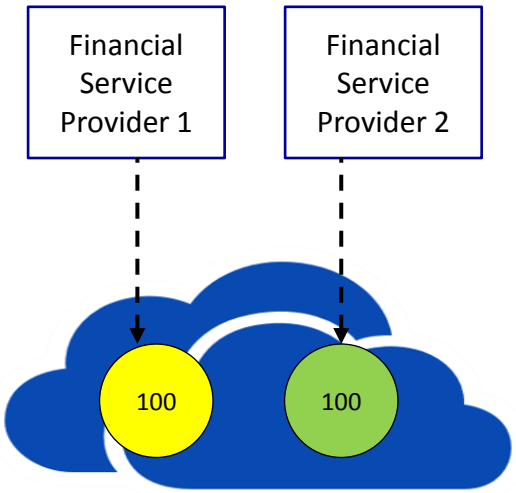
Collaborative Cloud Audit Group designed to enable cloud adoption in the financial industry and to maximise efficiency

Key challenges in cloud adaption when outsourcing regulated workload

- Additional technical risks [e.g. multi-tenant isolation]
- Jurisdiction
- **Agreement and enforcement of unrestricted audit rights relevant to regulator(s) and internal audit of the outsourcer**
- Data protection
- Systematic risk concentration with the cloud vendor
- Vendor lock-in/ portability

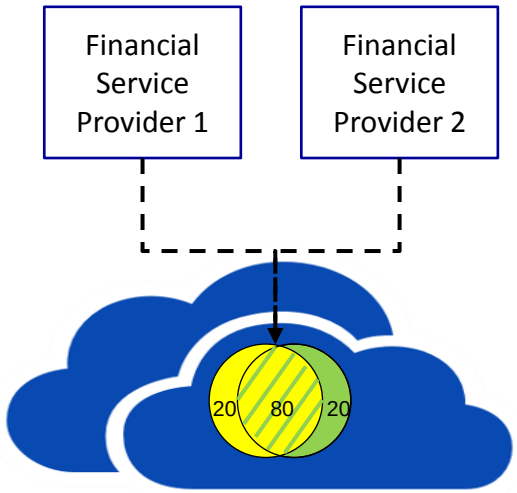
Core idea: Collaborative audit group to execute unrestricted audit rights

Individual audit scope



Effort
Vendor: 100 + 100 = **200**
Outsourcer: **100**

Collaborative audit scope



Effort
Vendor: 20 + 20 + 80 = **120**
Outsourcer: **20** + small collaboration group share

- Maximises efficiency and effectiveness
- Based on audit best-practices
- Executes individual audit rights in a group format

Focus of group audit on “security OF the cloud”

Managed by Customer

Optimized Network/OS/App Controls

Service-specific Controls

Cross-service Controls

API

Cloud Service Provider (CSP) Controls

Managed by CSP

Security ***IN*** the cloud

- *Securing access*
- *Defining User / Roles / Policies*
- *Data protection*
- *Logging & monitoring*
- *…*

Security ***OF*** the cloud

- *Datacentre compound*
- *Physical hardware / network*
- *Up to hypervisor level*
- *CSP platform & services*
- *Access management*
- *CSP staff*

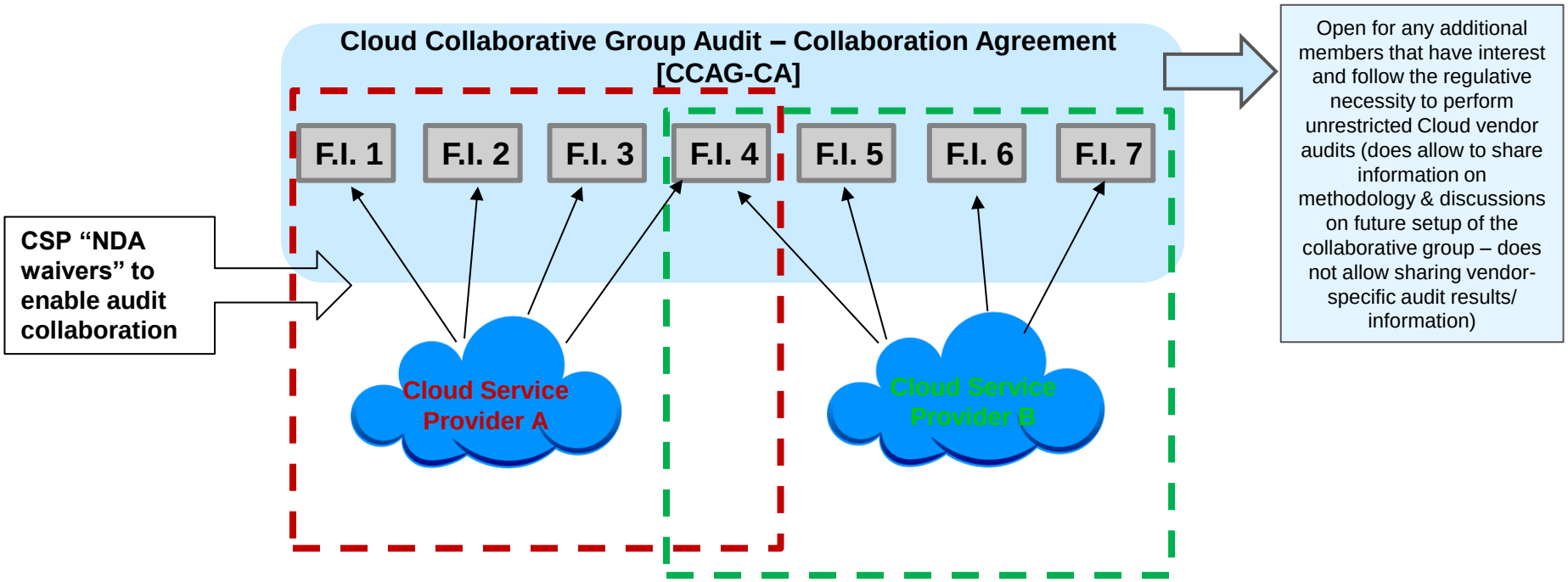
☐ Focus of collaborative audit group

Cornerstones of the group audit on Microsoft cloud

Active engagement of legal & audit pre-requisite

- "**Real audit**" and not a "second pilot audit"
- Scope focus on **Microsoft Azure** in a first step, preparation for **O365** audit in a second step (depending esp. also on the audit capacity availabilities)
- Usage of "**Crew Members only**" – meaning every financial institution which wants to participate needs to nominate at **least one dedicated Auditor and Legal contact**
- No contracting of a 3rd party audit firm on behalf of the "whole group", no "audit outsourcing"; **focus on the internal audit teams** of the Crew Members, Crew Members may individually leverage their audit capacities with 3rd party auditors performing audit tasks under the direction of the Crew Member and under the coordination of the audit team leadership
- **Collaborative Audit Group approach remains completely open** for regulated financial institutions which may want to join the respective audits due to their interest in using Cloud Services. Prioritization and timing of Cloud Service Provider ("CSP") audits driven by demand of audit group, available internal audit capacity, and CSP capacity & readiness (e.g. CSP must have granted respective audit rights beforehand). Group can also decide to start further parallel CSP audits in parallel as soon as respective demand is there
- Setup of **comprehensive contractual framework** for protection and disclosure of confidential information
- Pre-requisite for audit apart of audit & legal capacity is an existing **business relation** with the CSP & respective unrestricted **audit rights**
- Each financial institution to **cover it's own costs** and plan for respective (travel) budget

Structural setup of Collaborative Cloud Audit Group



Corner stones:

1. Fully transparent open-access approach: Open to any additional cloud vendors and regulated financial institutions that have unrestricted audit rights by the respective vendors - focus is collaboration in performing joint Cloud audits
2. After alignment of very high-level scope & timing, open invitation to interested financial institutions to join the respective audit
3. CCAG-Collaboration Agreement is contractual basis for general collaboration amongst audit group members – underneath the CCAG-CA the subset of financial institutions which perform a particular group together agree on scope and capacity in a separate „Project Collaboration Agreement" (PCA)
4. CSP grants audit group members a „NDA waiver" which enables collaboration and information sharing in the audit context
5. Audit group consists of auditors which prepare and conduct the audit in a joint format
6. All detailed audit plans, evidences, and reports are completely shared within the audit group, so that each auditor/ institution can make up it's own independent and fair opinion – no outsourcing of core audit activities/ responsibilities
7. Responsibility & risk to perform and evaluate audit (results) stays with the respective company

Core steps to join the audit group and perform joint audits

#	Who?	Does what?
0	Audit group & CSP	Agree on general roles and responsibilities, audit expectations, very high-level audit scope and time frame & openly inform and invite for group audit
1	Financial institution	Ensures availability of necessary audit rights bilateral with CSP
2	Financial institution	Ensures availability of sufficient own capacity/ resources to join the group audit (audit & legal)
3	Financial institution	Contacts audit group coordinator/ contract administrator to join the group, receives the accession request and joins the collaborative cloud audit group - collaboration agreement (CCAG-CA)
4	Audit Group Coordinator	Informs CSP on audit group members and receives confirmation from CSP that they do have the audit right
5	CSP	Provides „NDA waivers“ towards audit group members which registered for the specific audit
6	Audit Group	Agrees on „Project Collaboration Agreement“ (PCA) for particular audit
7	Audit Group	Aligns on most severe risks, prioritizes audit scope, prepares detailed audit plan
8	Audit Group	Informs CSP officially about the detailed audit scope, timing, and audit participants with an „audit start letter“ and initial document request
9	Audit Group & CSP	Align on logistical details for audit fieldwork
10	Audit Group & CSP	Audit Fieldwork: Audit conduction, remote audit work, on-site inspections of data & operation centres
11	Audit Group	Collection of evidences, preparation of factual observation report
12	Audit Group & CSP	Alignment of factual correctness of observations
13	Audit Group	Final audit report send to CSP
14	Financial institution	Evaluation and interpretation of audit observations according to individual risk profile and business needs
15	Financial Institution or Group	Follow-up with CSP on potential observation mitigations

Collaborative Cloud Audit Group - Members

Pilot Audit Group/ PoC on AWS H2 2017

"Crew members"

BERENBERG PRIVATBANKIERS SEIT 1590

UniCredit

DEUTSCHE BÖRSE GROUP

"Passengers"

Deutsche Bank

pbb DEUTSCHE PFANDBRIEFBANK

hannover re®

solarisBank

Schwäbisch Hall Auf diese Steine können Sie bauen

VOLKSWAGEN FINANCIAL SERVICES THE KEY TO MOBILITY

DEUTSCHE WERTPAPIERTREUHAND

Pilot Audit/ PoC organized with "crew members" who performed formed the subset performing the actual audit fieldwork and "passengers" who contributed in the overall concept development and high-level scope alignment

Audit Group/ Audit on Microsoft Azure H1 2018

"Crew members only"

ABN·AMRO

BERENBERG PRIVATBANKIERS SEIT 1590

COMMERZBANK

Mercedes-Benz Bank

Munich RE

UniCredit

hannover re®

pbb DEUTSCHE PFANDBRIEFBANK

DEUTSCHE BÖRSE GROUP

SIEMENS

Siemens Financial Services

Subset of group which currently performs the MS Azure audit

Audit Group open format to conduct Cloud Audits in a collaborative format. Accessible to all regulated financial institutions. Particular audits are performed by a subset of the group and announced open upfront to allow all interested financial institutions to join

Status and next steps

Background:

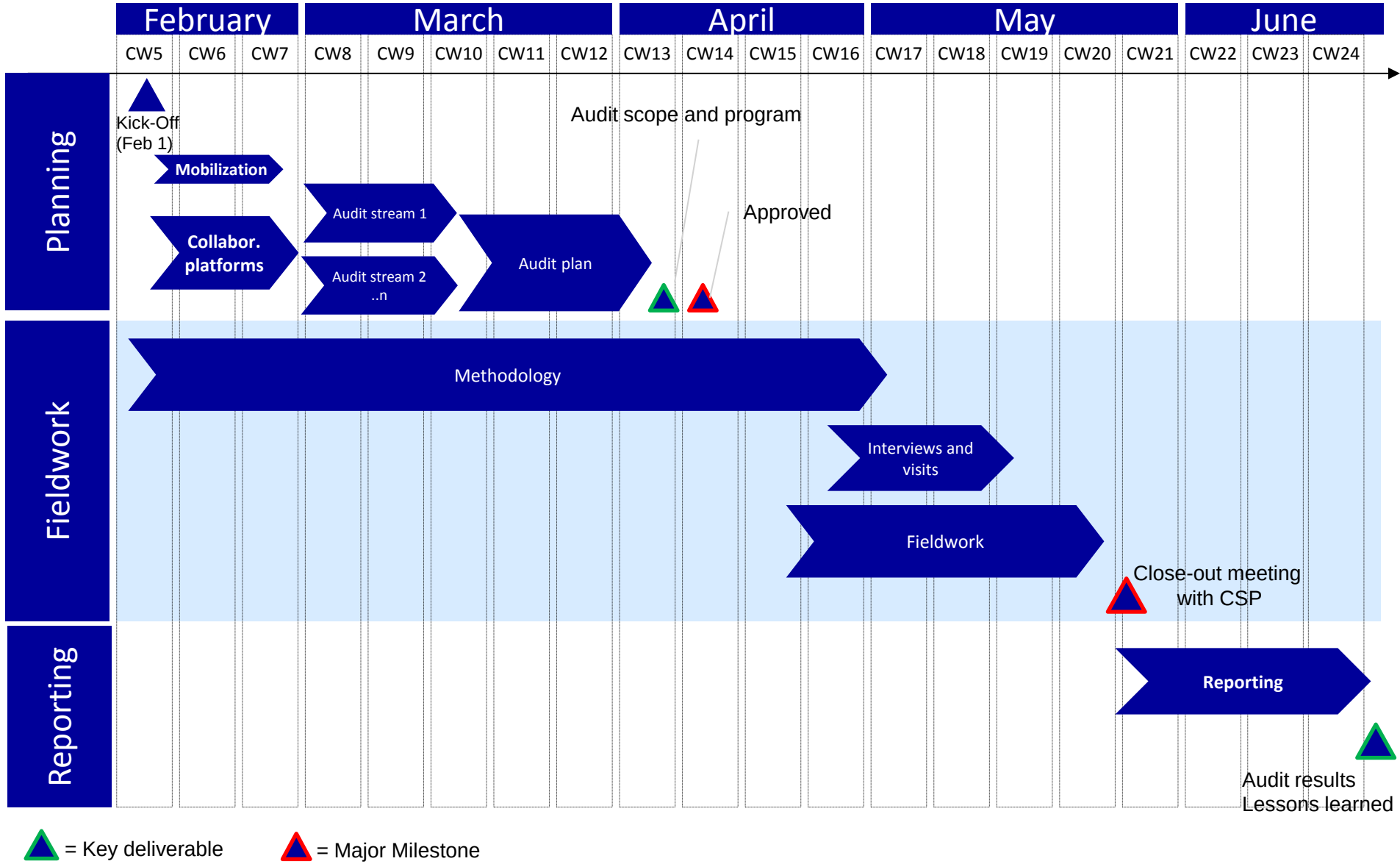
- Collaborative audit group initiated in June 2017
- Pilot audit conducted in H2/2017 on AWS – confirmed viability of collaborative audit format
- Group decision to conduct first “real” audit on Microsoft taken in November 2017
  [Microsoft Azure as first audit priority, followed by Microsoft Office 365]
- Open call for interest/participation on December 18, 2017

Timeline for Microsoft Azure group audit:

- By 31 JAN 2018 — Financial Institutions which want to join the “Microsoft Azure Group Audit” to nominate their respective Internal Audit & Legal contact
- 01 FEB 2018 — Kick-off workshop [10am-4pm CET]
- ~FEB-APR 2018 — Preparation of group audit based on legal basis
- ~APR-JUL 2018 — Audit fieldwork & report
  [*timing depending on progress of preparation phase and of legal basis*]

High-level plan time-plan

Currently slightly delayed by ~2-3 weeks



Thank you very much for your attention! Questions?

Michael Girg, Chief Cloud Officer
Tel: +49 69 211-15929
Michael.Girg@deutsche-boerse.com

Bastian Bahnemann, Executive Office
Tel: +49 69 211-17049
Bastian.Bahnemann@deutsche-boerse.com

Simmons & Simmons

simmons-simmons.com
elexica.com