

Presentation to PhUSE EU Connect
2018

Cloud Services -
A Framework for Adoption in the
Regulated Life Sciences Industry

November 2018

Anders Vidstrup -
Senior IT Quality
SME, NNIT A/S



Agenda

- Background
- Key issues
- Next steps



Background

- 2013/2014: Team formation, brainstorming, case-studies -> framework concept
- Three versions of concept paper submitted
- Version 4 is under revision, including appendices on:
 - Cloud Terminology
 - Cloud Audit Activities
 - Cloud Case Stories
 - Regulatory requirements and Cloud Solutions

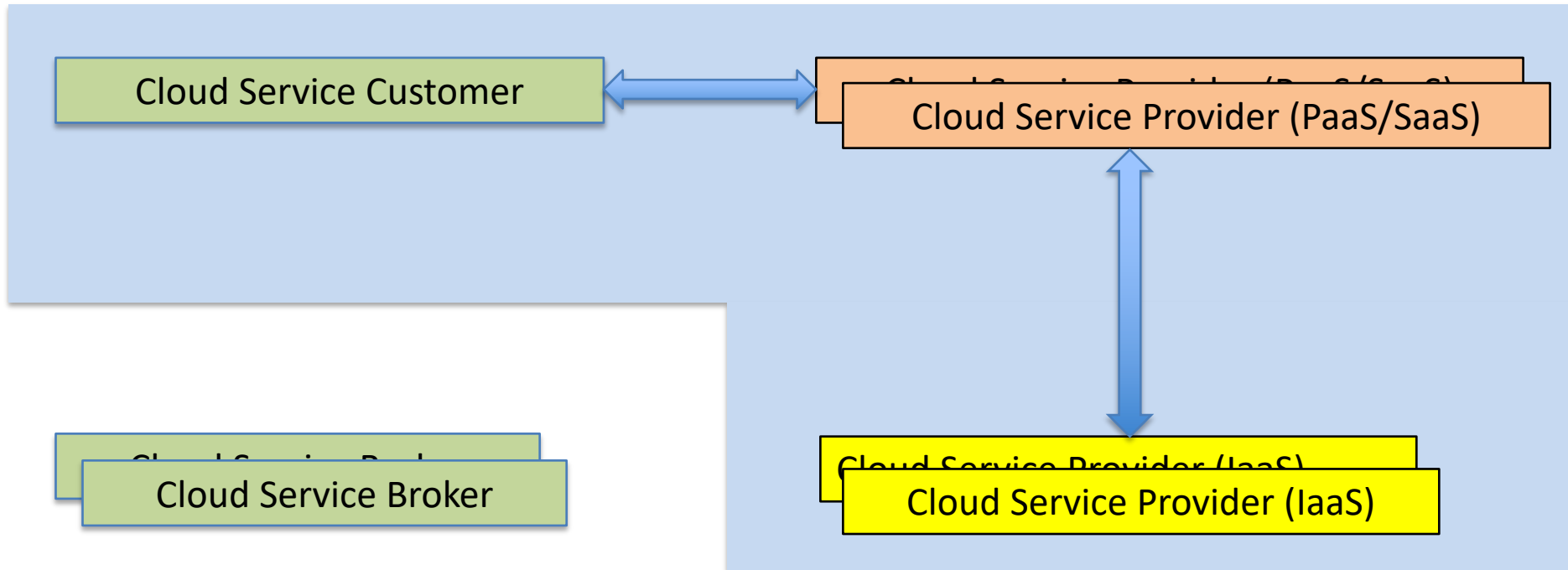


4 Key Roles

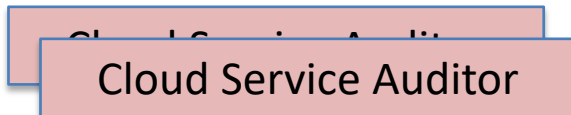
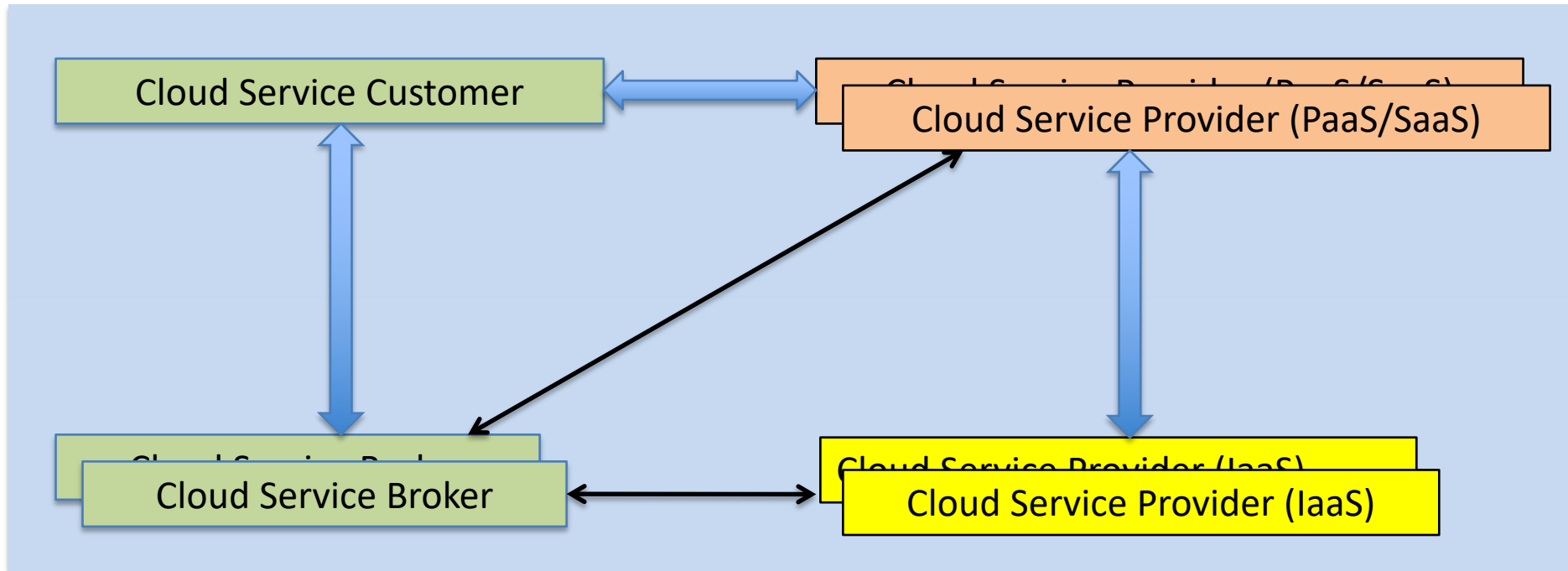
- **Cloud Service Customer:** In the context of GxP, these are generally the organizations or entities that purchase/use the cloud services to support their GxP-regulated activities. They are generally billed for the cloud services they consume, and depending on the services requested (IaaS, PaaS, SaaS), their activities, use cases and GxP requirements may vary.
- **Cloud Service Provider:** Organizations or entities responsible for providing cloud services to customers. The activities that the cloud providers perform will vary depending on their particular service offerings and can include building, deploying, operating and maintaining the cloud apps, infrastructure and associated service layers.
- **Cloud Service Broker:** These are the organizations or entities that manage the configuration, delivery and use of cloud services on behalf of the cloud customer. For example, cloud managers may perform infrastructure change control activities on the infrastructure built using general purpose, commercial cloud services.
- **Cloud Auditor:** A cloud auditor is a party that is qualified to conduct assessments of the cloud provider and the cloud infrastructure underlying the IaaS, PaaS, SaaS services. The auditor may be an independent third party such as a third party assessment organization (3PAO) or can also be a member of the consumer, provider or manager organization.



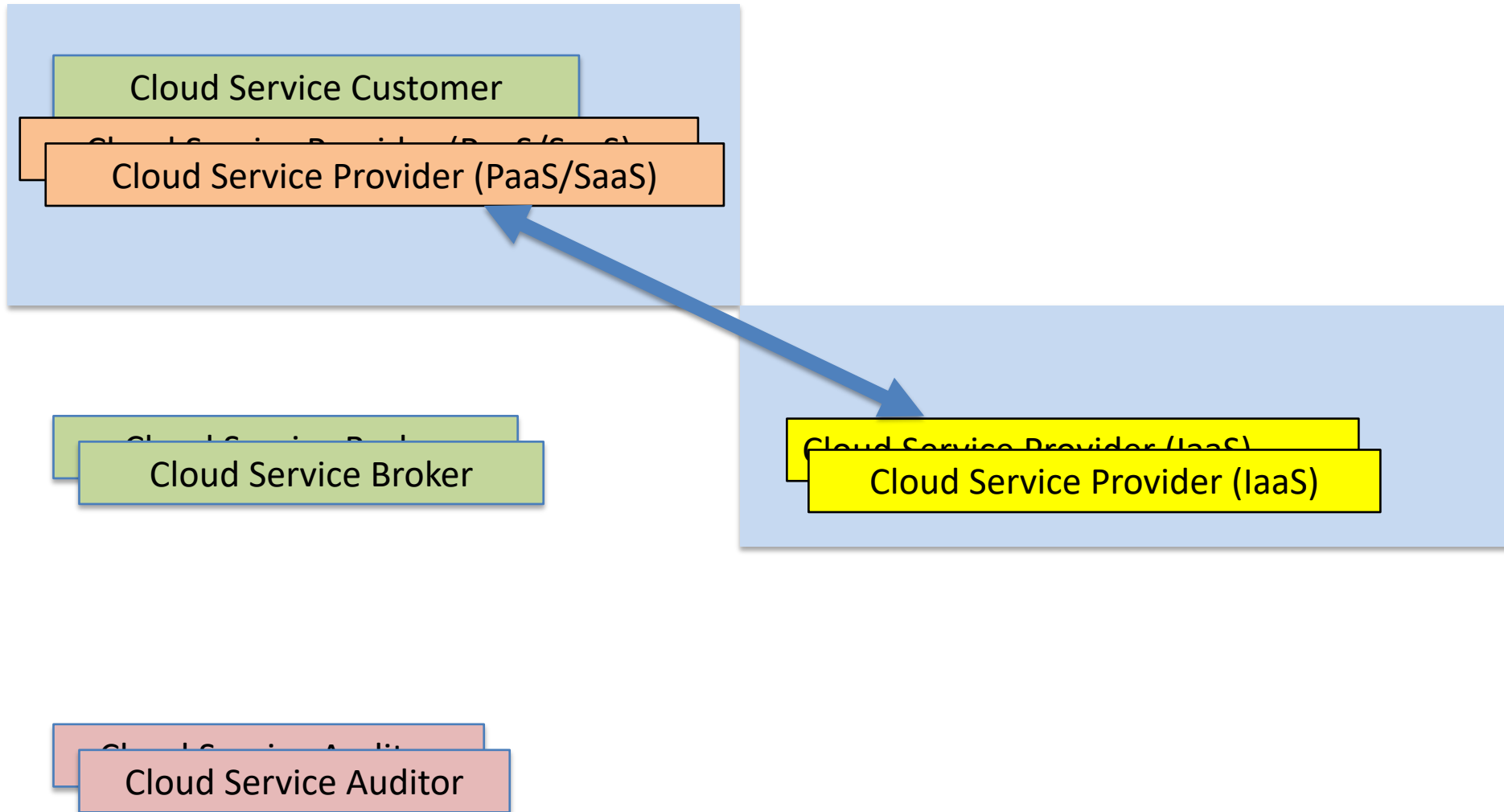
Cloud “Supply Chains”



Cloud “Supply Chains”



Cloud “Supply Chains”



Key issues right now

- Availability of data, and data integrity
- Facilitating compliance with GxP predicate rules in relation to supplier assessment/audits
- Contract with cloud service provider
- Inspection readiness



Availability of data, and data integrity

- Data Loss and Data Breaches. Who's liable for damages from interruptions in service?
- Malicious Insiders; How can users avoid vendor lock-in and exit if needed?
- Insure interfaces and API's
- Where is the data actually going to be physically located?
- Change Management. What happens when providers decide to change their service?

Very often
SOC2 and
other security
related reports
are provided



Supplier assessment/audits

- Often a SOC2/ISO 27001 report is provided – but:
 - ISO 9001 is the international standard that ***specifies requirements for a quality management system*** (QMS).
 - ISO 27001 specifies a management system that is intended to bring ***information security under management control and gives specific requirements***.



ISO 9001 and 27001

- There is a difference between a quality approach and a security approach.
- The following clauses from ISO 9001:2015 are not covered by ISO27001:2013 or there are no similar clauses in ISO 27001:
 - Quality management principles (Introduction, clause 0.2)
 - Process approach (Introduction, clause 0.3)
 - Customer focus (Leadership, clause 5.1.2)
 - People (Support, clause 7.1.2)
 - Infrastructure (Support, clause 7.1.3)
 - Environment for the operation of processes (Support, clause 7.1.4)
 - Monitoring and measuring resources (Support, clause 7.1.5)
 - Organisational knowledge (Support, clause 7.1.6)
 - Release of products and services (Operation, clause 8.6)
 - Control of nonconforming outputs (Operation, clause 8.7)
- Even though there is an overlap between the two standards, there is still a need for e.g. defining quality metrics, quality management review etc.



Inspection readiness

- Quality responsible is the same independent of outsourcing or using cloud solutions.
- It is expected to have support under inspections if needed. Following to be aware of together with Cloud Service Provider
 - Can documentation be provided, and how.
 - Competency in answering an investigator's questions
 - Do the regulated company have a set-up to handle long distance support from the Cloud Service Provider
- How to handle inspection at Cloud Service Provider site?
- Prepare questions for:
 - Data location
 - Access control
 - Back-up
 - How contracts are monitored.



Next step

- Framework document in version 4 under final revision.
- Appendices on:
 - Cloud Terminology – close to be ready for internal review
 - Cloud Audit Activities – under final revision
 - Cloud Case Stories – we might need input
 - Regulatory requirements and Cloud Solutions – close to be ready for internal review



Thank you for your attention

Questions?



The premier community for people working in the biometric area



@PhUSETwitta



PhUSE



www.phusewiki.org